GS-2724

Ethernet Switch

User's Guide

Version 3.70
4/2007
Edition 1

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the GS-2724 using the web configurator or via commands. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

✎ It is recommended you use the web configurator to configure the Switch.

- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The GS-2724 may be referred to as the "Switch", the "device", the "system" or the "product" in this User's Guide.
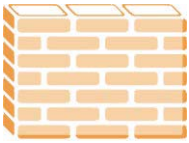- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch	Computer	Notebook computer
Server	DSLAM	Firewall
Telephone	Switch	Router

5

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- The length of exposed (bare) power wire should not exceed 7mm.

This product is recyclable. Dispose of it properly.

Contents Overview

Table of Contents

12

List of Figures

List of Tables

29

PART I

Introduction and Hardware

Getting to Know Your Switch

This chapter introduces the main features and applications of the Switch.

1.1 Introduction

Your Switch is a stand-alone layer-3 Gigabit Ethernet switch. By integrating router functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching. The Switch has 20 Gigabit Ethernet ports and 4 GbE dual personality interfaces for uplink. A dual personality interface includes one Gigabit port and one slot for mini-GBIC transceiver (SFP module) with one port active at a time.

With its built-in web configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

See Appendix A on page 305 for a full list of software features available on the Switch.

1.1.1 Backbone Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1   Backbone Application
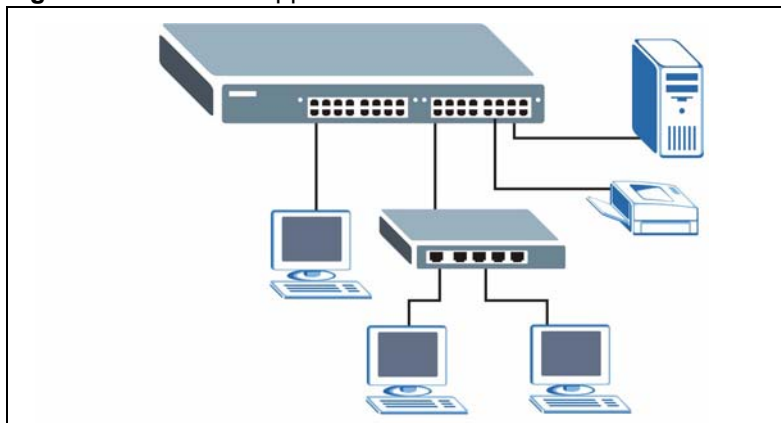
1.1.2 Bridging Example

In this example application the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using a Gigabit Ethernet/mini-GBIC port on the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 2   Bridging Application
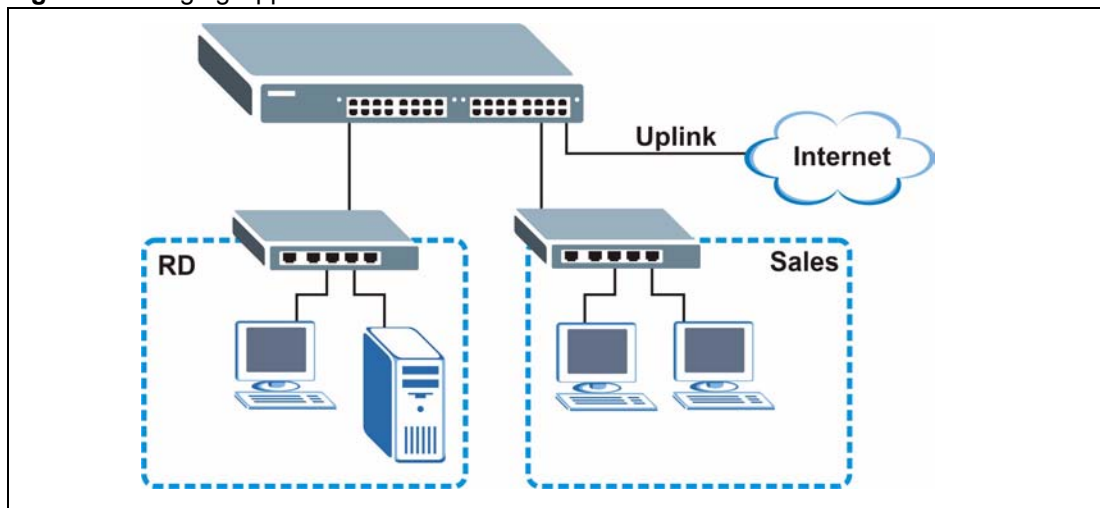
1.1.3 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use trunking to connect these two networks.

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance. The Switch can provide the same bandwidth as ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

Figure 3   High Performance Switched Workgroup Application
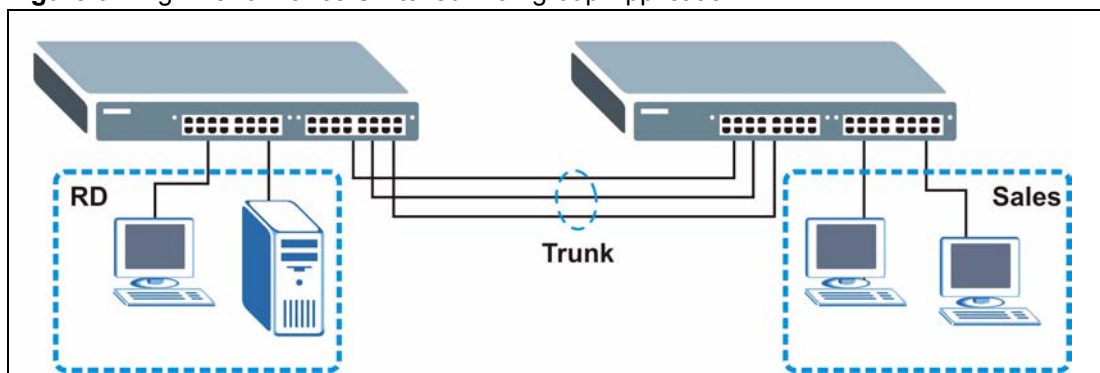
1.1.4 IEEE 802.1Q VLAN Application Examples

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

For more information on VLANs, refer to .

1.1.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4   Shared Server Using VLAN Example

35
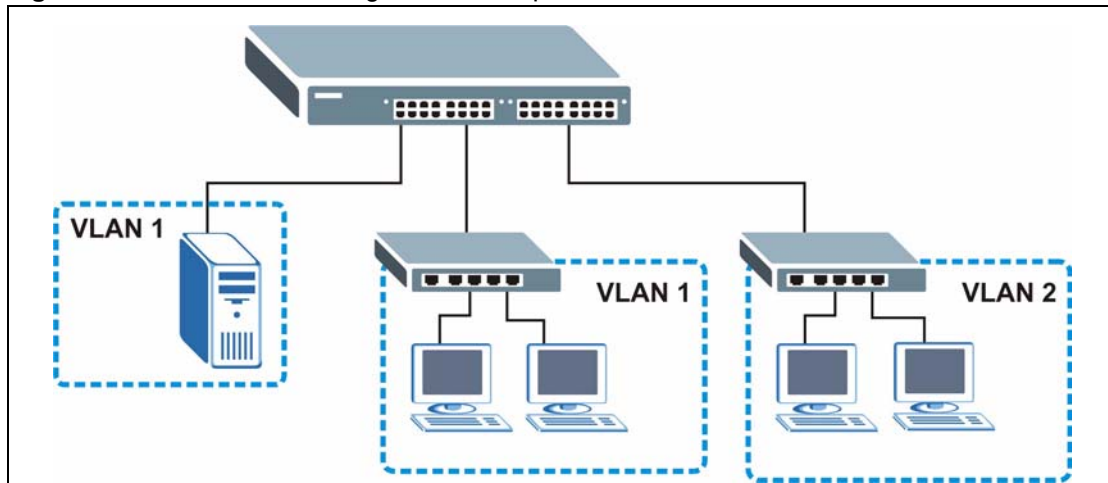
Hardware Installation and Connection

This chapter shows you how to install the hardware and make port connections.

✏️ Example graphics are shown.

2.1 Freestanding Installation

1 Make sure the Switch is clean and dry.
2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.
3 Make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord.
4 Remove the adhesive backing from the rubber feet.
5 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 5   Attaching Rubber Feet
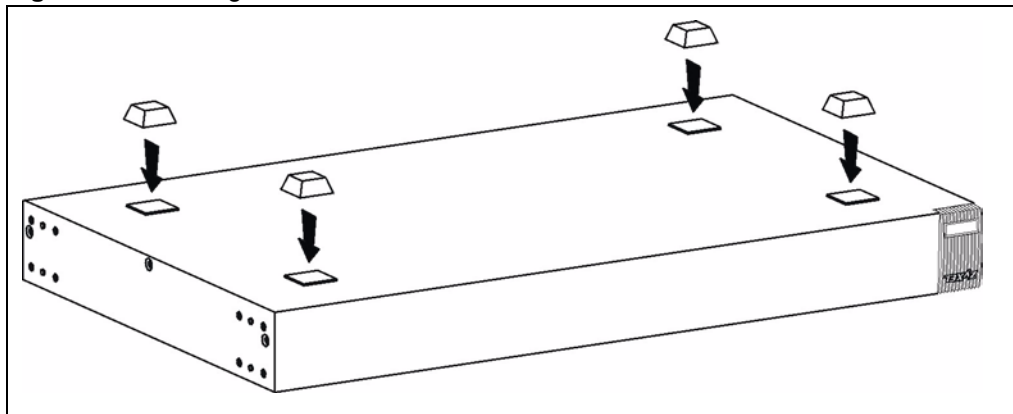
✍ Do NOT block the ventilation holes. Leave space between devices when stacking.

✍ For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the Switch. This is especially important for enclosed rack installations.

2.2 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.2.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

👁 Failure to use the proper screws may damage the unit.

2.2.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.2.2 Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.

Figure 6 Attaching the Mounting Brackets
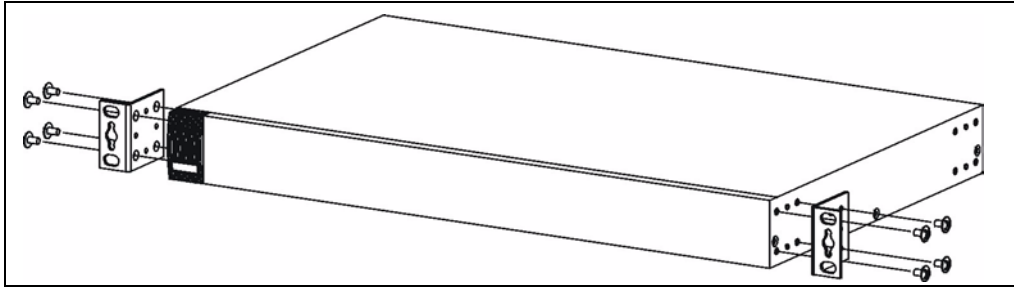
2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.

3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

4 You may now mount the Switch on a rack. Proceed to the next section.

2.2.3 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 7 Mounting the Switch on a Rack
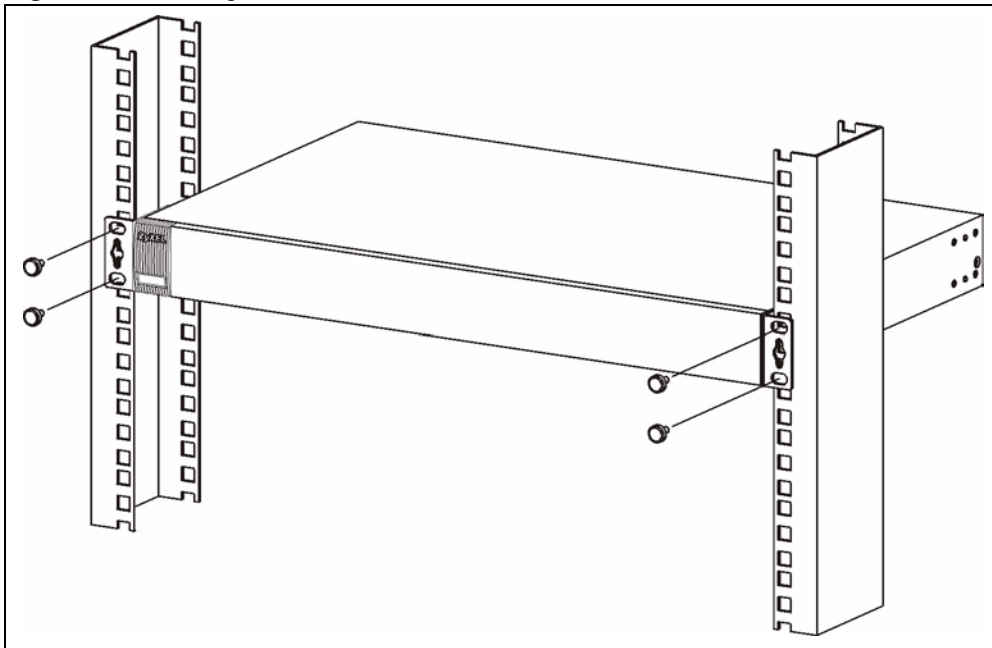
2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

Hardware Overview

This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

3.1 Front Panel Connection

The figure below shows the front panel of the Switch.

Figure 8   Front Panel
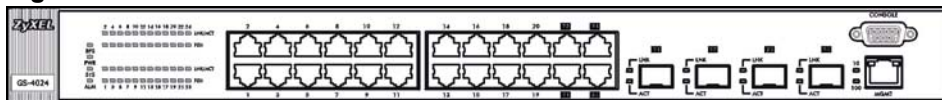
The following table describes the port labels on the front panel.

Table 1   Front Panel

PORT	DESCRIPTION
MGMT	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the Switch.
CONSOLE	Only connect this port if you want to configure the Switch using the command line interface (CLI) via the console port.
20 100/1000 Mbps RJ-45 Gigabit Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch, or router.
Four Dual Personality Interfaces	Each interface has one 1000 Base-T copper RJ-45 port and one Small Form-Factor Pluggable (SFP) fiber port, with one port active at a time.
	• 4 100/1000 Mbps RJ-45 Gigabit Ports: Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches.
	• 4 Mini‑GBIC Ports: Use mini‑GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches (see Section 3.1.3 on page 42 for instructions).

3.1.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps

- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Gigabit Ethernet Ports

The Switch has 10/100/1000 Mbps auto-negotiating, auto-crossover Gigabit Ethernet ports. In 10/100/1000 Mbps Gigabit Ethernet, the speed can be 10 Mbps, 100 Mbps or 1000 Mbps and the duplex mode can be half duplex (for 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the Switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: on

3.1.3 SFP Slots

The Switch comes with SFP (Small Form-factor Pluggable) slots for mini-GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Switch does not come with transceivers. You must use transceivers that comply with the SFP transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

SFP transceivers can be standalone interfaces or part of a dual personality interface. Each dual personality interface has one 1000 Base-T copper RJ-45 port and one Small Form-Factor Pluggable (SFP) fiber slot for mini-GBIC transceivers, with one port active at a time. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

To avoid possible eye injury, do NOT look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

Use the following steps to install a mini-GBIC transceiver (SFP module).

1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

Figure 9 Transceiver Installation Example
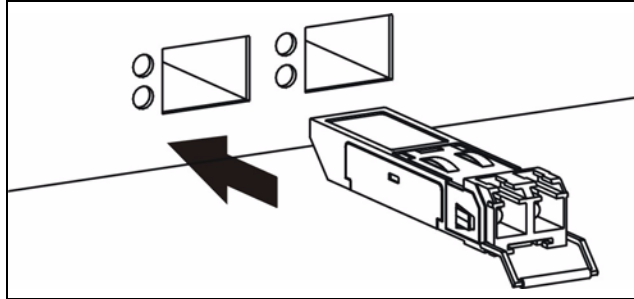
2 Press the transceiver firmly until it clicks into place.

3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 10 Installed Transceiver
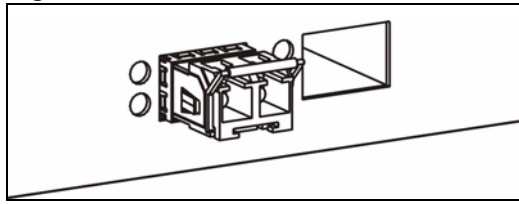
3.1.3.2 Transceiver Removal

Use the following steps to remove a mini-GBIC transceiver (SFP module).

1 Open the transceiver's latch (latch styles vary).

Figure 11 Opening the Transceiver's Latch Example
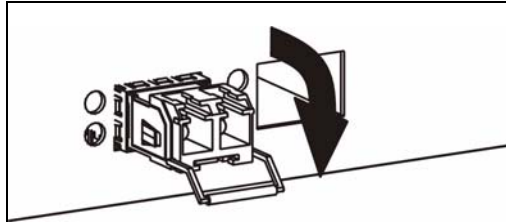
2 Pull the transceiver out of the slot.

Figure 12 Transceiver Removal Example
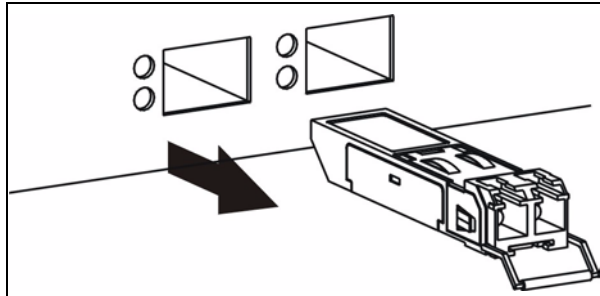
3.2 Rear Panel

The following figures show the rear panels of the AC and DC models. The rear panel contains a connector for backup power supply (BPS) and the power receptacle. For the DC model, it also contains the power switch.

Figure 13 Rear Panel: AC Model
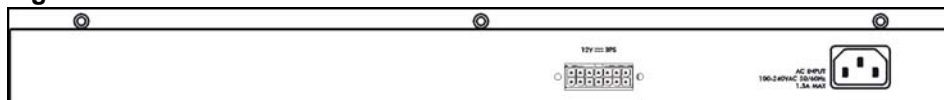
Figure 14 Rear Panel: DC Model

3.2.1 Power Connector

Make sure you are using the correct power source as shown on the panel.

To connect the power to the AC model, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to a 100~240V AC, 1.5A power outlet. Make sure that no objects obstruct the airflow of the fans.

The DC model requires DC power supply input of -48 VDC to -60 VDC, 1.6A max, no tolerance. To connect the power to the DC model, insert one end of the supplied power cord to the power receptacle on the rear panel and the other end to a power outlet. Make sure that no objects obstruct the airflow of the fans.

3.2.2 External Backup Power Supply Connector

The backup power supply constantly monitors the status of the internal power supply. The backup power supply automatically provides power to the Switch in the event of a power failure. Once the Switch receives power from the backup power supply, it will not automatically switch back to using the internal power supply even when the power is resumed.

3.3 LEDs

The following table describes the LEDs.

Table 2 LEDs

LED	COLOR	STATUS	DESCRIPTION
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
PWR	Green	On	The system is turned on.
		Off	The system is off.

Table 2 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
Gigabit Ethernet Ports			
LNK/ACT	Green	On	The port has a successful 10/1000 Mbps connection.
	Amber	On	The port has a successful 100 Mbps connection.
		Blinking	The port is sending or receiving data.
		Off	The port is disconnected or the link failed.
FDX	Amber	On	The port is in full duplex mode.
		Blinking	The port detected a collision event.
		Off	The port is in half duplex mode or there is no connection.
Mini-GBIC (SFP) Slots			
LNK	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data or there is no connection.
MGMT Port			
10	Green	On	The link to a 10 Mbps Ethernet network is up.
		Blinking	The port is sending or receiving data at 10 Mbps.
		Off	The link to a 10 Mbps Ethernet network is down.
100	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The port is sending or receiving data at 100 Mbps.
		Off	The link to a 100 Mbps Ethernet network is down.
Gigabit Ethernet Ports (Part of Dual Personality Interface)			
1000	Green	Blinking	The port is sending/receiving data.
		On	The link to a 10/1000 Mbps Ethernet network is up.
		Off	The link to a 10/1000 Mbps Ethernet network is down.
100	Amber	Blinking	The port is sending/receiving data.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to a 100 Mbps Ethernet network is down.

PART II

Basic Configuration

47

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

1 Start your web browser.
2 Type "http://" and the IP address of the Switch (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].
3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 15 Web Configurator: Login

4   Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

Figure 16 Web Configurator Home Screen (Status)
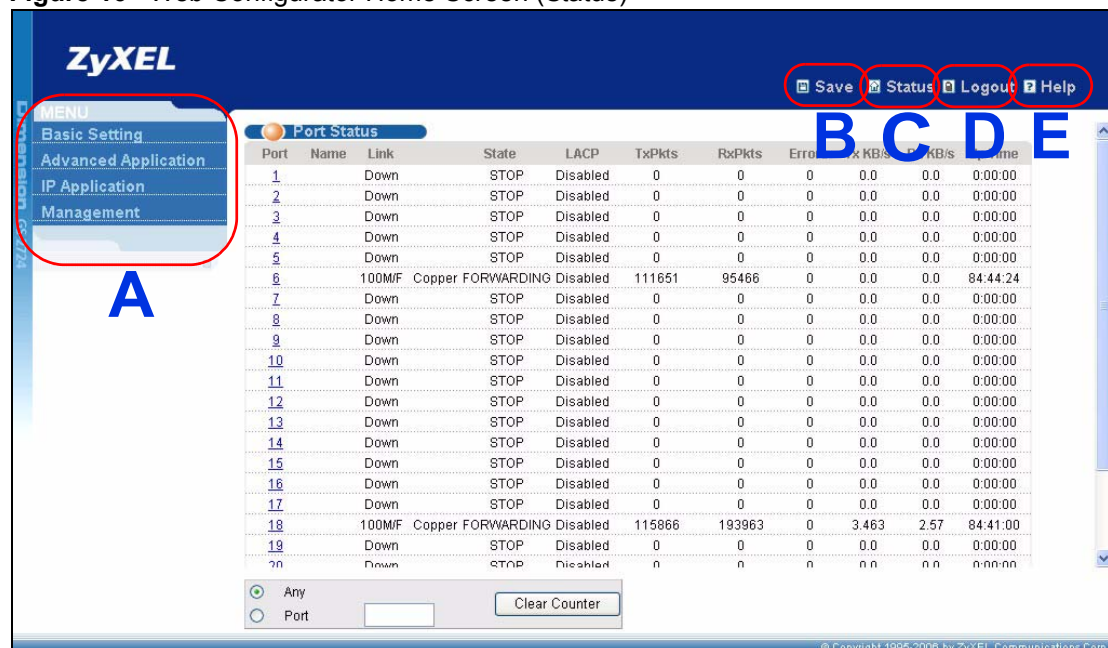
A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, **C**, **D**, **E** - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.
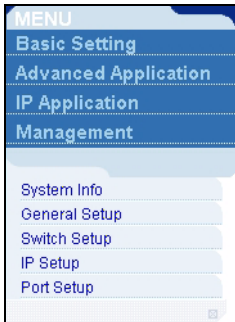
C - Click this link to go to the status page of the Switch.

D - Click this link to logout of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 3 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
MENU Basic Setting Advanced Application IP Application Management System Info General Setup Switch Setup IP Setup Port Setup	MENU Basic Setting Advanced Application IP Application Management VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Authentication Port Security Classifier Policy Rule Queuing Method VLAN Stacking Multicast	MENU Basic Setting Advanced Application IP Application Management Static Routing RIP IGMP DiffServ DHCP	MENU Basic Setting Advanced Application IP Application Management Maintenance Access Control Diagnostic Syslog Cluster Management MAC Table IP Table ARP Table Routing Table Configure Clone

The following table lists the various web configurator screens within the sub-links.

Table 4 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT

System Info
General Setup
Switch Setup
IP Setup
Port Setup
	VLAN
	   VLAN Status
	   VLAN Port Setting
	   Static VLAN
	Static MAC Forwarding
	Filtering
	Spanning Tree Protocol
	   Status
	   Spanning Tree
	   Protocol Configuration
	Bandwidth Control
	Broadcast Storm Control
	Mirroring
	Link Aggregation
	   Status
	   RSTP
	   MRSTP
	Port Authentication
	   RADIUS
	   802.1x
	Port Security
	Classifier
	Policy Rule
	Queuing Method
	VLAN Stacking
	Multicast
	   Setting
	   Status
	   IGMP Filtering Profile
	   MVR
	   Group Configuration
		Static Routing
		RIP
		IGMP
		DiffServ
		   DSCP Setting
		DHCP Server Status
		   DHCP Server
		   DHCP Relay
			Maintenance
			   Firmware Upgrade
			   Restore Configuration
			   Backup Configuration
			   Load Factory Default
			   Save Configuration
			   Reboot System
			Access Control
			   SNMP
			   Logins
			   Service Access Control
			   Remote Management
			Diagnostic
			Syslog
			   Syslog Setup
			   Syslog Server Setup
			Cluster Management
			   Status
			   Configuration
			MAC Table
			IP Table
			ARP Table
			Routing Table
			Configure Clone

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to screens where you can configure settings for individual Switch ports.
Advanced Application	

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to a screen where you can configure VLAN stacking.
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
IP Application	
Static Routing	This link takes you to screens where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
RIP	This link takes you to a screen where you can configure the RIP (Routing Information Protocol) direction and versions.
IGMP	This link takes you to a screen where you can configure the IGMP settings.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to a screen where you can configure the DHCP settings.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).

Table 5   Navigation Panel Links (continued)

LINK	DESCRIPTION
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
IP Table	This link takes you to a screen where you can view the IP addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **Access Control > Logins** to display the next screen.

Figure 17   Change Administrator Login Password

4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Use **the Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

1 Delete the management VLAN (default is VLAN 1).
2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
3 Filter all traffic to the CPU port.
4 Disable all ports.
5 Misconfigure the text configuration file.
6 Forget the password and/or IP address.
7 Prevent all services from accessing the Switch.
8 Change a service port number but forget it.

Be careful not to lock yourself and others out of the Switch. If you do lock yourself out, try using out-of-band management (via the management port) to configure the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

1 Connect to the console port using a computer with terminal emulation software. See for details.

2 Disconnect and reconnect the Switch's power to begin a session. When you reconnect the Switch's power, you will see the initial screen.

3 When you see the message "`Press any key to enter Debug Mode within 3 seconds ...`" press any key to enter debug mode.

4 Type `atlc` after the "`Enter Debug Mode`" message.

5 Wait for the "`Starting XMODEM upload`" message before activating XMODEM upload on your terminal.

6 After a configuration file upload, type `atgo` to restart the Switch.

Figure 18 Resetting the Switch: Via the Console Port

```
Bootbase Version: V3.1 | 03/08/2007 18:22:24
RAM:Size = 64 Mbytes
DRAM POST: Testing: 65536K OK
DRAM Test SUCCESS !
FLASH: Intel 64M

ZyNOS Version: V3.70(AYC.0)b0 | 03/08/2007 14:39:15

Press any key to enter debug mode within 3 seconds.
..............................................................
     (Compressed)
     Version: GS-2724, start: 500e9030
     Length: A37326, Checksum: 2411
     Compressed Length: 22F7C8, Checksum: CA3C




Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:19:cb:00:11:f9
initialize switch, ethernet address: 00:19:cb:00:11:fa
Initializing switch unit 0...
Initializing switch unit 1...
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Press ENTER to continue...
```

The Switch is now reinitialized with a default configuration file including the default password of "1234".

4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 19   Web Configurator: Logout Screen

Thank you for using the Web Configurator.
Please close the browser before next login.
Goodbye!

4.8 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

Initial Setup Example

This chapter shows how to set up the Switch for an example network.

5.1 Overview

The following lists the configuration steps for the example network:

- Configure an IP interface
- Configure DHCP server settings
- Create a VLAN
- Set port VLAN ID
- Enable RIP

5.1.1 Configuring an IP Interface

On a layer-3 switch, an IP interface (also known as an IP routing domain) is not bound to a physical port. The default IP address of the Switch is 192.168.1.1 with a subnet mask of 255.255.255.0.

In the example network, since the **RD** network is already in the same IP interface as the Switch, you don't need to create an IP interface for it. However, if you want to have the **Sales** network on a different routing domain, you need to create a new IP interface. This allows the Switch to route traffic between the **RD** and **Sales** networks.

Figure 20   Initial Setup Network Example: IP Interface
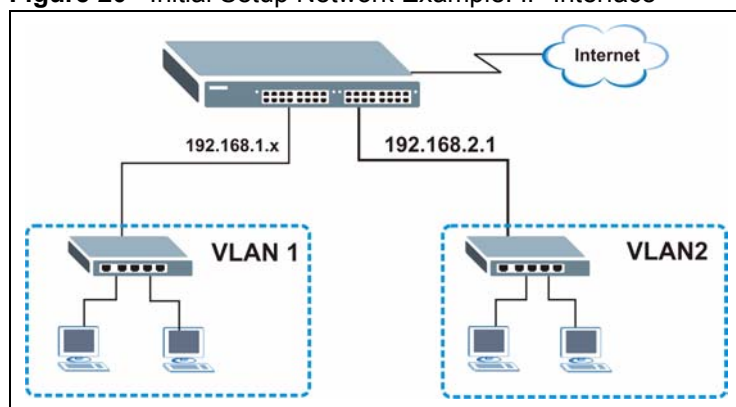
1   Connect your computer to the **MGMT** port that is used only for management. Make sure your computer is in the same subnet as the **MGMT** port.

2 Open your web browser and enter 192.168.0.1 (the default **MGMT** port IP address) in the address bar to access the web configurator. See Section 4.2 on page 49 for more information.

3 Click **Basic Setting** and **IP Setup** in the navigation panel.

4 Configure the related fields in the **IP Setup** screen.

For the **Sales** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

5 In the **VID** field, enter the ID of the VLAN group to which you want this IP interface to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

6 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.2 Configuring DHCP Server Settings

You can set the Switch to assign network information (such as the IP address, DNS server, etc.) to DHCP clients on the network.

For the example network, configure two DHCP client pools on the Switch for the DHCP clients in the **RD** and **Sales** networks.

1 In the web configurator, click **IP Application** and **DHCP** in the navigation panel and click the **Server** link.

2 In the **DHCP Server** screen, specify the ID of the VLAN to which the DHCP clients belong, the starting IP address pool, subnet mask, default gateway address and the DNS server address(es).

3 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.3 Creating a VLAN

VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

Figure 21   Initial Setup Network Example: VLAN
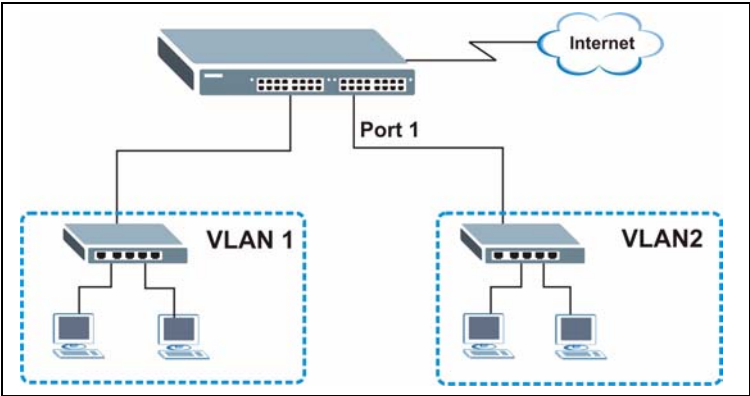
1 Click **Advanced Application** and **VLAN** in the navigation panel and click the **Static VLAN** link.

2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.

61

✎ The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.
5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.4 Setting Port VID

Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

Figure 22   Initial Setup Network Example: Port VID
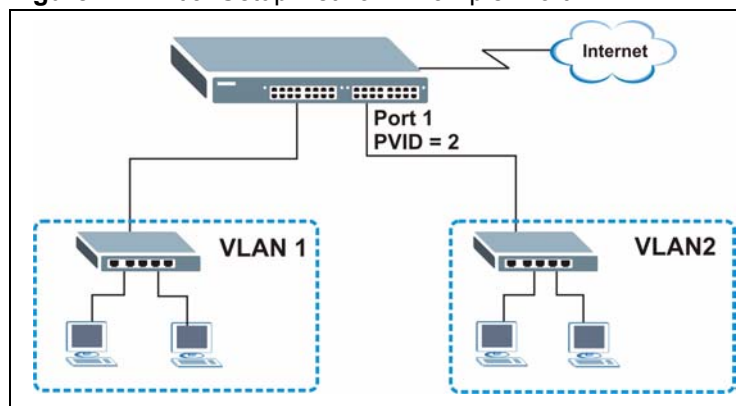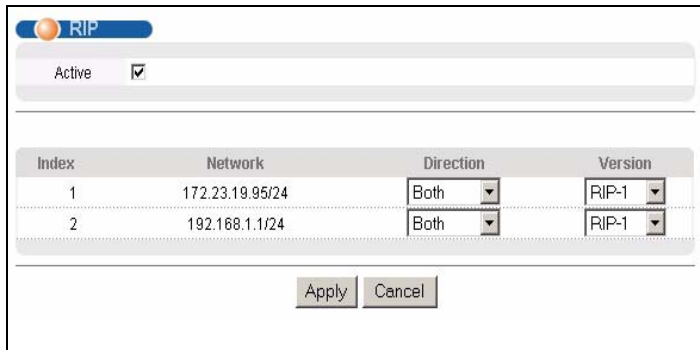
1 Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.
2 Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.1.5 Enabling RIP

To exchange routing information with other routing devices across different routing domains, enable RIP (Routing Information Protocol) in the **RIP** screen.

1 Click **IP Application** and **RIP** in the navigation panel.

2 Select **Both** in the **Direction** field to set the Switch to broadcast and receive routing information.

3 In the **Version** field, select **RIP-1** for the RIP packet format that is universally supported.

4 Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

63

System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.
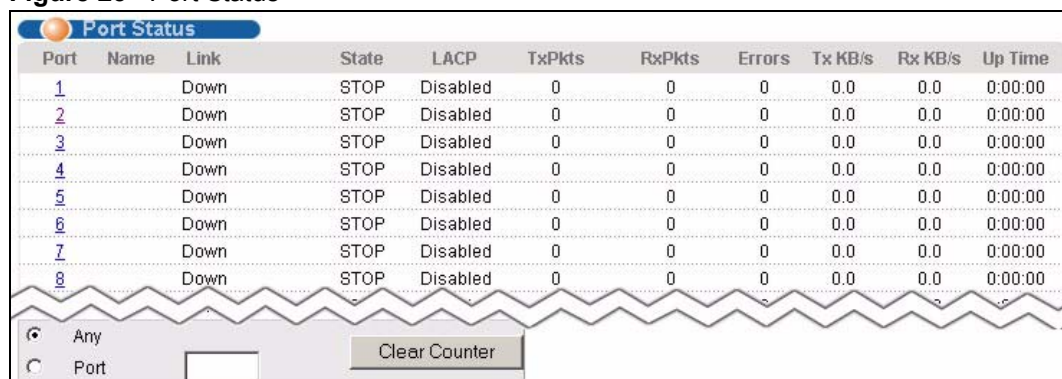
6.1 Overview

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

6.2 Port Status Summary

To view the port statistics, click **Status** in any web configurator screen to display the **Status** screen as shown next.

Figure 23   Port Status

The following table describes the labels in this screen.

Table 6   Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 24 on page 67).
Name	This is the name you assigned to this port in the **Basic Setting**, **Port Setup** screen.

Table 6 Port Status (continued)

LABEL	DESCRIPTION
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1 on page 101 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Enter a port number and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

6.2.1 Status: Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 24   Port Details

The following table describes the labels in this screen.

Table 7   Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**).
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1 on page 101 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.

Table 7 Port Details (continued)

LABEL	DESCRIPTION
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about packets transmitted.	
TX Packet	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packet	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.

Table 7 Port Details (continued)

LABEL	DESCRIPTION
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

69

Basic Setting

This chapter describes how to configure the **System Info, General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

7.1 Overview

The **System Info** screen displays general information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your Switch. The real time is then displayed in the logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure the Switch's IP address in each routing domain, subnet mask(s) and DNS (domain name server) for management purposes.

7.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number and monitor the Switch's temperature, fan speeds and voltage in this screen.

Figure 25 System Info

The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
ZyNOS F/W Version	This field displays the version number of the Switch's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**MAC**, **CPU** and **PHY** refer to the location of the temperature sensors on the Switch's printed circuit board.
Current	This shows the current temperature in degrees centigrade at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.

Table 8 System Info (continued)

LABEL	DESCRIPTION
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

7.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** > **General Setup** in the navigation panel to display the screen as shown.

Figure 26   General Setup

The following table describes the labels in this screen.

Table 9   General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Login Precedence	Use this drop-down list box to select which database the Switch should use (first) to authenticate an administrator (user for Switch management).
	Configure the local user accounts in the **Access Control Logins** screen. The RADIUS is an external server. Before you specify the priority, make sure you have set up the corresponding database correctly first.
	Select **Local Only** to have the Switch just check the administrator accounts configured in the **Access Control Logins** screen.
	Select **Local then RADIUS** to have the Switch check the administrator accounts configured in the **Access Control Logins** screen. If the user name is not found, the Switch then checks the user database on the specified RADIUS server. You need to configure **Port Authentication Radius** first.
	Select **RADIUS Only** to have the Switch just check the user database on the specified RADIUS server for a login username, password and the access privilege.

Table 9 General Setup (continued)

LABEL	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format, it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). The Switch requests time and date settings from the time server in the following circumstances: • When the Switch starts up. • In 24-hour intervals after starting up. • When you click **Apply** in this screen. **None** is the default value. Enter the time manually. When you enter the time settings manually, the Switch uses the new settings when you click **Apply**. Each time you turn on the Switch, the time and date will be reset to the default values.
Time Server IP Address	Enter the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

7.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

✎ VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 8 on page 85 for information on port-based and 802.1Q tagged VLANs.

7.5 Switch Setup Screen

Click **Basic Setting** > **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

Figure 27   Switch Setup

The following table describes the labels in this screen.

Table 10 Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See Chapter 8 on page 85for more information.
Bridge Control Protocol Transparency	Select **Active** to allow the Switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the **Port Setup** screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Time sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. Leave Time must be two times larger than **Join Timer**; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

Table 10 Switch Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

7.6 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains. To open this screen, click **Basic Setting > IP Setup**.

7.6.1 IP Interfaces

The Switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

On the Switch, as a layer-3 device, an IP address is not bound to any physical ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

You can configure multiple routing domains on the same VLAN as long as the IP address ranges for the domains do not overlap. To change the IP address of the Switch in a routing domain, simply add a new routing domain entry with a different IP address in the same subnet.

Figure 28 IP Setup

The following table describes the labels in this screen.

Table 11 IP Setup

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (**In-Band** or **Out-of-band**) the Switch is to send packets originating from itself (such as SNMP traps) or packets with unknown source. Select **Out-of-band** to have the Switch send the packets to the management port labelled **MGMT**. This means that device(s) connected to the other port(s) do not receive these packets. Select **In-Band** to have the Switch send the packets to all ports except the management port (labelled **MGMT**) to which connected device(s) do not receive these packets.
Management IP Address	Use these fields to set the settings for the out-of-band management port.

Table 11 IP Setup (continued)

LABEL	DESCRIPTION
IP Address	Enter the out-of-band management IP address of your Switch in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.0.254
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
IP Interface	Use these fields to create or edit IP routing domains on the Switch.
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation. For example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Delete	Click **Delete** to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out from the Switch.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.7 Port Setup

Use this screen to configure the Switch's port settings. Click **Basic Setting** > **Port Setup** in the navigation panel to display the configuration screen.

Figure 29 Port Setup

The following table describes the labels in this screen.

Table 12 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This field displays **10/100/1000M** for Gigabit connections.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **100M/Full Duplex** and **1000M/Full Duplex**. Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

Table 12   Port Setup (continued)

LABEL	DESCRIPTION
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port.
	The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.
	IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.
	Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 10 on page 77 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the **Switch Setup** screen first.
	Select **Peer** to process any BPDU (Bridge Protocol Data Units) received on this port.
	Select **Tunnel** to forward BPDUs received on this port.
	Select **Discard** to drop any BPDU received on this port.
	Select **Network** to process a BPDU with no VLAN tag and forward a tagged BPDU.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

PART III
Advanced

83

VLAN

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

8.1 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

8.1.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

8.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

8.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

8.2.1.1 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

8.2.2 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 13 IEEE 802.1Q VLAN Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/ deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member

8.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking,** you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

Figure 30   Port VLAN Trunking
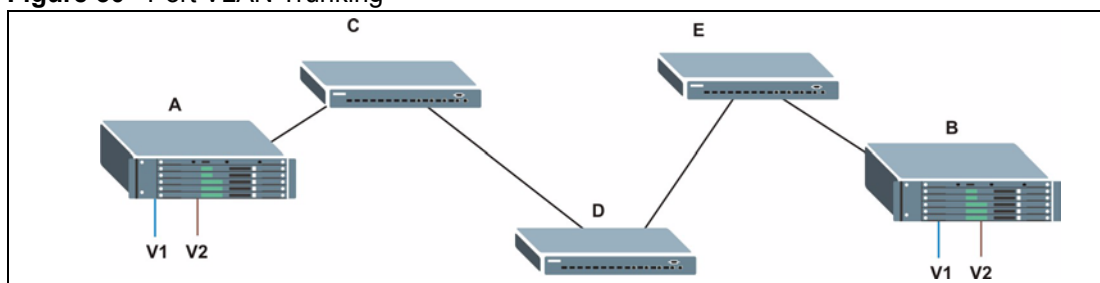
8.4 Select the VLAN Type

Select a VLAN type in the **Switch Setup** screen.

Figure 31   Switch Setup: Select VLAN Type

87

8.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

• sent to a VLAN group as normal depending on its VLAN tag.
• sent to a group whether it has a VLAN tag or not.
• blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

8.5.1 Static VLAN Status

See Section 8.1 on page 85 for more information on Static VLAN. Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 32   VLAN Status

The following table describes the labels in this screen.

Table 14   VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the Switch.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. **dynamic**: using GVRP **static**: added as a permanent entry **other**: added in another way, such as via Multicast VLAN Registration (MVR).
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 Static VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See Section 8.1 on page 85 for more information on static VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 33 VLAN Detail

The following table describes the labels in this screen.

Table 15 VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. **dynamic**: using GVRP **static**: added as a permanent entry **other**: added in another way, such as via Multicast VLAN Registration (MVR).

8.5.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. See Section 8.1 on page 85 for more information on static VLAN. To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 34 Static VLAN

The following table describes the related labels in this screen.

Table 16 Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.

Table 16   Static VLAN (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.5.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See Section 8.1 on page 85 for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 35   VLAN Port Setting

The following table describes the labels in this screen.

Table 17   VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local switch.
Port Isolation	**Port Isolation** allows each port to communicate only with the CPU management port and the dual personality GbE interfaces but not communicate with each other. This option is the most limiting but also the most secure.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	Enter a number between 1and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

8.6 Port-based VLAN Setup

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.

✎ When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

✎ In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

8.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen and then click **Advanced Application > VLAN** from the navigation panel to display the next screen.

Figure 36   Port Based VLAN Setup (All connected)

Figure 37 Port Based VLAN Setup (Port isolation)

The following table describes the labels in this screen.

Table 18 Port Based VLAN Setup

label	Description
Setting Wizard	Choose **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.

Table 18 Port Based VLAN Setup (continued)

label	Description
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

9.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

9.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See Chapter 17 on page 127 for more information on port security.

Click **Advanced Applications > Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 38   Static MAC Forwarding

The following table describes the labels in this screen.

Table 19 Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

Filtering

This chapter discusses MAC address port filtering.

10.1 Configure a Filtering Rule

Filtering means sifting traffic going through the Switch based on the source and/or destination MAC addresses and VLAN group (ID).

Click **Advanced Application** > **Filtering** in the navigation panel to display the screen as shown next.

Figure 39 Filtering

The following table describes the related labels in this screen.

Table 20 Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.

Table 20 Filtering (continued)

LABEL	DESCRIPTION
Action	Select **Discard source** to drop frame from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

Spanning Tree Protocol

The Switch supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

11.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

> ✎ In this user's guide, "STP" refers to both STP and RSTP.

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 21 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

11.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 22 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.1.4 Multiple RSTP

MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.

✎ Each port can belong to one STP tree only.

Figure 40 MRSTP Network Example
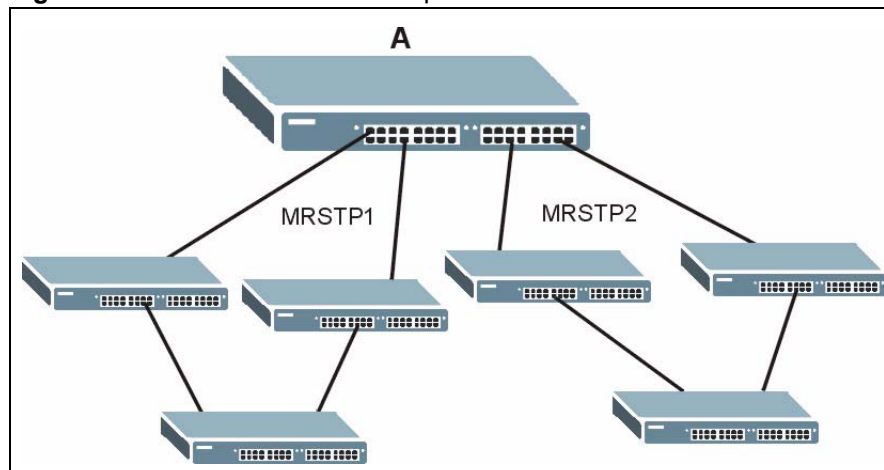
11.2 Spanning Tree Protocol Main Screen

The Switch allows you to configure a single RSTP configuration or you can configure multiple configurations. See Section 11.1 on page 101 for more information on RSTP. Click **Advanced Application**, **Spanning Tree Protocol** in the navigation panel to choose whether you want to configure multiple or a single Spanning Tree Protocol configuration.

✎ This screen is only available if neither RSTP or MRSTP is active. Once you select RSTP or MRSTP this screen displays the status of your configuration.

Figure 41   Spanning Tree Protocol

The following table describes the labels in this screen.

Table 23   Spanning Tree Protocol

LABEL	DESCRIPTION
RSTP	This link takes you to the Rapid Spanning Tree Protocol configuration screen. See Section 11.3 on page 104.
MRSTP	This link takes you to the Multiple Rapid Spanning Tree Protocol configuration screen. See Section 11.5 on page 107.

11.3 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 11.1 on page 101 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 42 Rapid Spanning Tree Protocol

The following table describes the labels in this screen.

Table 24 Rapid Spanning Tree Protocol

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 43 on page 107).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The Switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Table 24   Rapid Spanning Tree Protocol (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost-see Table 21 on page 102 for more information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

11.4 Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1 on page 101 for more information on RSTP.

✎   This screen is only available after you activate RSTP on the Switch.

Figure 43   Rapid Spanning Tree Protocol Status

The following table describes the labels in this screen.

Table 25   Rapid Spanning Tree Protocol Status

LABEL	DESCRIPTION
Configuration	Click **Configuration** to configure RSTP settings. Refer to Section 11.3 on page 104.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time**, **Max Age** and **Forwarding Delay**
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.5 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, select **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1 on page 101 for more information on MRSTP.

Figure 44 Multiple Rapid Spanning Tree Protocol

The following table describes the labels in this screen.

Table 26 Multiple Rapid Spanning Tree Protocol

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen (see Figure 43 on page 107).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Table 26   Multiple Rapid Spanning Tree Protocol (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost-see Table 21 on page 102 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

11.6 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1 on page 101 for more information on MRSTP.

✍ This screen is only available after you activate MRSTP on the Switch.

Figure 45 Multiple Rapid Spanning Tree Protocol Status

The following table describes the labels in this screen.

Table 27 Multiple Rapid Spanning Tree Protocol Status

LABEL	DESCRIPTION
Configuration	Click **Configuration** to configure MRSTP settings. Refer to Section 11.3 on page 104.
Tree	Select which STP tree configuration you want to view.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time**, **Max Age** and **Forwarding Delay**
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

12

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

12.1 Bandwidth Control Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows on a port.

12.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

✎   **The CIR should be less than the PIR. The sum of CIRs cannot be greater than or equal to the uplink bandwidth.**

12.2 Bandwidth Control Setup

Click **Advanced Application** > **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 46 Bandwidth Control

The following table describes the related labels in this screen.

Table 28 Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

13.1 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

Click **Advanced Application** > **Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 47   Broadcast Storm Control

The following table describes the labels in this screen.

Table 29 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Mirroring

This chapter discusses port mirroring setup screens.

14.1 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Advanced Application** > **Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 48   Mirroring

115

The following table describes the labels in this screen.

Table 30   Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Enter the port number of the monitor port.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

15.1 Link Aggregation Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

15.2 Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The Switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 31   Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

Table 32   Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

15.3 Link Aggregation Control Protocol Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Control Protocol Status screen** displays by default. See Section 15.1 on page 117 for more information.

Figure 49   Link Aggregation Control Protocol Status

The following table describes the labels in this screen.

Table 33   Link Aggregation Control Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.2.1 on page 118 for more information on this field.

---

1.   Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

Table 33 Link Aggregation Control Protocol Status (continued)

LABEL	DESCRIPTION
Enabled Port	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.

15.4 Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Control Protocol Status** screen to display the screen shown next. See Section 15.1 on page 117 for more information on link aggregation.

Figure 50   Link Aggregation

119

The following table describes the labels in this screen.

Table 34 Link Aggregation

LABEL	DESCRIPTION
Link Aggregation Control Protocol	
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.
Dynamic (LACP)	Select this check box to enable LACP for a trunk.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Group	Select the trunk group to which a port belongs.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup. See Section 40.9 on page 278 for information on how to use the commands to configure additional Radius server settings as well as multiple Radius server configuration.

16.1 Port Authentication Overview

IEEE 802.1x is an extended authentication protocol[2] that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.

16.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

Figure 51   RADIUS Server
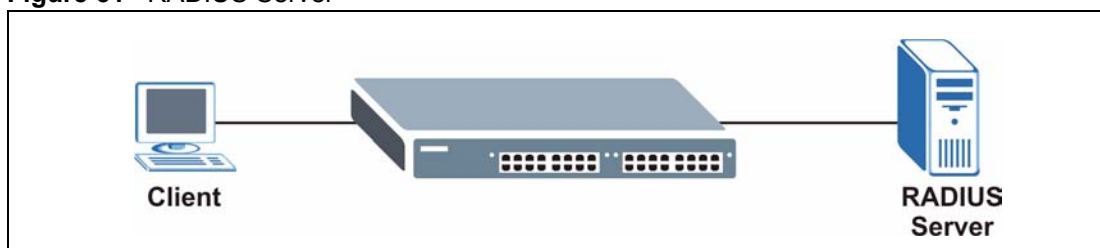
16.1.1.1 Vendor Specific Attribute

A Vendor Specific Attribute (VSA) is an attribute-value pair that is sent between a RADIUS server and the Switch. Configure VSAs on the RADIUS server to set the Switch to perform the following actions on an authenticated user:

- Limit bandwidth on incoming or outgoing traffic
- Assign account privilege levels

---

2. At the time of writing, only Windows XP of the Microsoft operating systems supports it. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

> ✎ Refer to the documentation that comes with your RADIUS server on how to configure a VSA.

The following table describes the VSAs supported on the Switch.

Table 35   Supported VSA

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	`Vendor-Id = `**`890`**` (ZyXEL)` `Vendor-Type = `**`1`** `Vendor-data = ` ingress rate (decimal)
Egress Bandwidth Assignment	`Vendor-Id = `**`890`**` (ZyXEL)` `Vendor-Type = `**`2`** `Vendor-data = ` egress rate (decimal)

Privilege Assignment	`Vendor-ID = `**`890`**` (ZyXEL)`
	`Vendor-Type = `**`3`**
	`Vendor-Data = `**`"shell:priv-lvl=N"`**
	or
	`Vendor-ID = `**`9`**` (CISCO)`
	`Vendor-Type = `**`1`**` (CISCO-AVPAIR)`
	`Vendor-Data = `**`"shell:priv-lvl=N"`**
	where `N` is a privilege level (from 0 to 14).
	
	Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

16.1.1.2 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server to assign a port on the Switch to a VLAN (fixed, untagged). This will also set the port's VID. Refer to RFC 3580 for more information.

Table 36   Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	`Tunnel-Type = `**`VLAN(13)`** `Tunnel-Medium-Type = `**`802(6)`** `Tunnel-Private-Group-ID = ` VLAN ID Note: You must also create a VLAN with the specified VID on the Switch.

16.2 Port Authentication Configuration

To enable port authentication, first activate IEEE802.1x security (both on the Switch and the port(s)) then configure the RADIUS server settings.

Click **Advanced Application** > **Port Authentication** in the navigation panel to display the screen as shown.

Figure 52 Port Authentication

16.2.1 Configuring RADIUS Server Settings

Use this screen to configure your RADIUS server settings. See Section 16.1.1 on page 121 for more information on RADIUS servers. From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown.

Figure 53 RADIUS

The following table describes the labels in this screen.

Table 37 RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

16.2.2 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. From the **Port Authentication** screen, click **802.1x** to display the configuration screen as shown.

Figure 54 802.1x

The following table describes the labels in this screen.

Table 38 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.

Table 38 802.1x (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Port Security

This chapter shows you how to set up port security.

17.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. See Appendix A on page 305 for the maximum number of MAC addresses the Switch can learn. There is no other limit on the maximum number of MAC addresses per port the Switch can learn, as long as the number of MAC addresses does not exceed the value in Appendix A on page 305.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

17.2 Port Security Setup

Click **Advanced Application** > **Port Security** in the navigation panel to display the screen as shown.

Figure 55   Port Security

The following table describes the labels in this screen.

Table 39   Port Security

LABEL	DESCRIPTION
Active	Select this option to enable port security on the Switch.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from "0" to "16384". "0" means this feature is disabled.

Table 39   Port Security (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Classifier

This chapter introduces and shows you how to configure the packet classifier on the Switch.

18.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

1 Configure classifiers to sort traffic into different flows.
2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to Chapter 19 on page 137 to configure policy rules).

18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to Chapter 19 on page 137.

Click **Advanced Application** > **Classifier** in the navigation panel to display the configuration screen as shown.

Figure 56 Classifier

The following table describes the labels in this screen.

Table 40 Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are **All**, **802.3 tagged**, **802.3 untagged**, **Ethernet II tagged** and **Ethernet II untagged**. A value of **802.3** indicates that the packets are formatted according to the IEEE 802.3 standards. A value of **Ethernet II** indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2 Specify the fields below to configure a layer 2 classifier.	
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.

Table 40 Classifier (continued)

LABEL	DESCRIPTION
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value. Refer to Table 42 on page 134 for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (**Any**).
Destination	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select **Other** and enter the protocol number in decimal value. Refer to Table 43 on page 135 for more information. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

✎ When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 57   Classifier: Summary Table

The following table describes the labels in this screen.

Table 41   Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 42   Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

Table 43   Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Classifier Example

The following screen shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

After you have configured a classifier, you can configure a policy (in the **Policy** screen) to define action(s) on the classified traffic flow.

Figure 58   Classifier: Example

Policy Rule

This chapter shows you how to configure policy rules.

19.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 18 on page 131 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to for more information.

Click **Advanced Applications** > **Policy Rule** in the navigation panel to display the screen as shown.

Figure 59   Policy

139

The following table describes the labels in this screen.

Table 44 Policy

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the **Classifier** screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the **Action** field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Type the number of an outgoing port.
Outgoing packet format for Egress port	Select **Tag** to add the specified VID to packets on the specified outgoing port. Otherwise, select **Untag**.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the Switch takes on the associated classified traffic flow.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets. Select **Do not drop the matching frame previously marked for dropping** to retain the frames that were marked to be dropped before.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1 priority** to replace the packet's 802.1 priority field with the value you set in the Priority field. Select **Send the packet to priority queue** to put the packets in the designated queue. Select **Replace the 802.1 priority field with the IP TOS value** to replace the packet's 802.1 priority field with the value you set in the **TOS** field.
Diffserv	Select **No change** to keep the TOS and/or DSCP fields in the packets. Select **Set the packet's TOS field** to set the TOS field with the value you configure in the **TOS** field. Select **Replace the IP TOS with the 802.1 priority value** to replace the TOS field with the value you configure in the **Priority** field. Select **Set the Diffserv Codepoint field in the frame** to set the DSCP field with the value you configure in the **DSCP** field.

Table 44 Policy (continued)

LABEL	DESCRIPTION
Outgoing	Select **Send the packet to the mirror port** to send the packet to the mirror port.
	Select **Send the packet to the egress port** to send the packet to the egress port.
	Select **Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port** to send the broadcast, multicast, DLF, marked-to-drop or CPU frames to the egress port.
	Select **Set the packet's VLAN ID** to set the VLAN ID of the packet with the value you configure in the **VLAN ID** field.
Metering	Select **Enable** to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic.
	Select **Drop the packet** to discard the out-of-profile traffic.
	Select **Change the DSCP value** to replace the DSCP field with the value specified in the **Out of profile DSCP** field.
	Select **Set Out-Drop Precedence** to mark out-of-profile traffic and drop it when network is congested.
	Select **Do not drop the matching frame previously marked for dropping** to queue the frames that are marked to be dropped.
Add	Click **Add** to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

19.3 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

Figure 60   Policy: Summary Table

Index	Active	Name	Classifier(s)	Delete
1	Yes	Test	Example;	☐

Delete   Cancel

The following table describes the labels in this screen.

Table 45   Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to).

Figure 61   Policy: Example

Queuing Method

This chapter introduces the queuing methods supported.

20.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

20.1.1 Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

20.1.2 Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

20.2 Configuring Queuing

Click **Advanced Application** > **Queuing Method** in the navigation panel.

Figure 62   Queuing Method

The following table describes the labels in this screen.

Table 46   Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	Select **SPQ** (Strict Priority Queuing) or **WRR** (Weighted Round Robin). Strict Priority Queuing (SPQ) services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q3 has the highest priority and Q0 the lowest. Weighted Round Robin Scheduling (WRR) services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Q0~Q7 Weight %	When you select **WRR,** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Calculate	Click **Calculate** to make sure the WFQ queuing weights total to 100%; if not an error message is displayed.

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your Switch. See the chapter on VLANs for more background information on Virtual LAN

21.1 VLAN Stacking Overview

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

21.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 63   VLAN Stacking Example
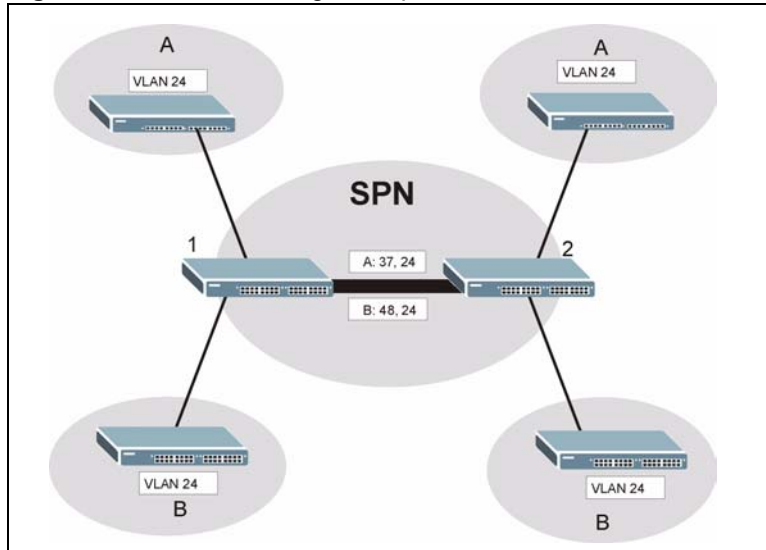
21.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking "roles", **Normal**, **Access Port** and **Tunnel** (the latter is for Gigabit ports only).

   • Select **Normal** for "regular" (non-VLAN stacking) IEEE 802.1Q frame switching.
   • Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.

> ✎ Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

   • Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by SP VID).

> ✎ Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

21.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 47 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the Switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the Switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the Switch. (If an incoming frame's **SP TPID** is the same as the one configured on the Switch, then the Switch will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

21.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as circled in the Switch's **VLAN Stacking** screen.

Table 48 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	**TPID**	**Priority**	**VID**	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	**SPTPID**	**Priority**	**VID**	TPID	**Priority**	**VID**	Len/Etype	Data	FCS	Double-tagged frame

Table 49 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

21.4 Configuring VLAN Stacking

Click **Advanced Applications** > **VLAN Stacking** to display the screen as shown.

Figure 64   VLAN Stacking

The following table describes the labels in this screen.

Table 50   VLAN Stacking

LABEL	DESCRIPTION
Active	Select this check box to enable VLAN stacking on the Switch.
SP TPID	**SP TPID** is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Choose **0x8100** or **0x9100** from the drop-down list box or select **Others** and then enter a four-digit hexadecimal number from 0x0000 to 0xFFFF. 0x denotes a hexadecimal number. It does not have to be typed in the **Others** text field.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 50 VLAN Stacking (continued)

LABEL	DESCRIPTION
Role	Select **Normal** to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in **SPVID** and **Priority** are ignored.
	Select **Access Port** to have the Switch add the **SP TPID** tag to all incoming frames received on this port. Select **Access Port** for ingress ports at the edge of the service provider's network.
	Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network.
	In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.
SPVID	**SPVID** is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 8 on page 85 for more background information on VLAN ID.
Priority	On the Switch, configure priority level of inner IEEE 802.1Q tag in the **Port Setup** screen. "0" is the lowest priority level and "7" is the highest.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Multicast

This chapter shows you how to configure various multicast features.

22.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways-Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group-it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

22.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

22.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

22.1.3 IGMP Snooping
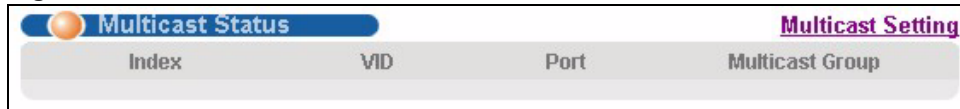
A switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

22.2 Multicast Status

Click **Advanced Applications** > **Multicast** to display the screen as shown. This screen shows the multicast group information. See Section 22.1 on page 153 for more information on multicasting.

Figure 65   Multicast Status

The following table describes the labels in this screen.

Table 51   Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

22.3 Multicast Setting

Click **Advanced Applications** > **Multicast** > **Multicast Setting** link to display the screen as shown. See Section 22.1 on page 153 for more information on multicasting.

Figure 66 Multicast Setting

The following table describes the labels in this screen.

Table 52 Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,711,450) in seconds. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.

155

Table 52 Multicast Setting (continued)

LABEL	DESCRIPTION
Reserved Multicast Group	Multicast addresses (224.0.0.0 to 224.0.0.255) are reserved for the local scope. For examples, 224.0.0.1 is for all hosts in this subnet, 224.0.0.2 is for all multicast routers in this subnet, etc. A router will not forward a packet with the destination IP address within this range. See the IANA web site for more information. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

22.4 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are allowed to join. A profile contains a range of multicast IP addresses (multicast groups) which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen, Section 22.3 on page 154). Clients connected to those ports are then permitted to join the multicast groups specified in the profile. Each port can be assigned a single profile only. A profile can be assigned to multiple ports.

Click **Advanced Applications** > **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** to display the screen as shown.

Figure 67 IGMP Filtering Profile

The following table describes the labels in this screen.

Table 53 IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes.
	To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile.
	If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click **Add** to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button.
	To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

157

22.5 MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

You must enable IGMP snooping to use MVR. However, MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 68   MVR Network Example
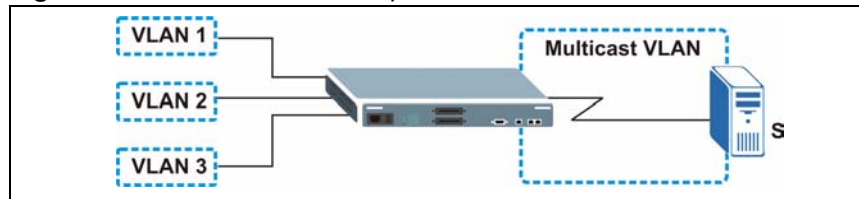
22.5.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

22.5.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

22.5.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 69   MVR Multicast Television Example
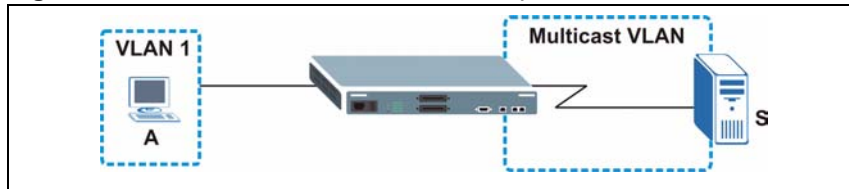
22.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications** > **Multicast** > **Multicast Setting** > **MVR** to display the screen as shown next.

> You can create up to three multicast VLANs and up to 256 multicast rules on the Switch.

> Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 70 MVR

The following table describes the related labels in this screen.

Table 54 MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.

Table 54   MVR (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

22.7 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 71 Group Configuration

The following table describes the labels in this screen.

Table 55 Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 22.1.1 on page 153 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to Section 22.1.1 on page 153 for more information on IP multicast addresses.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select **Delete Group** and click **Delete** to remove the selected entry(ies) from the table.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

22.7.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN are able to receive the traffic.

Figure 72   MVR Configuration Example
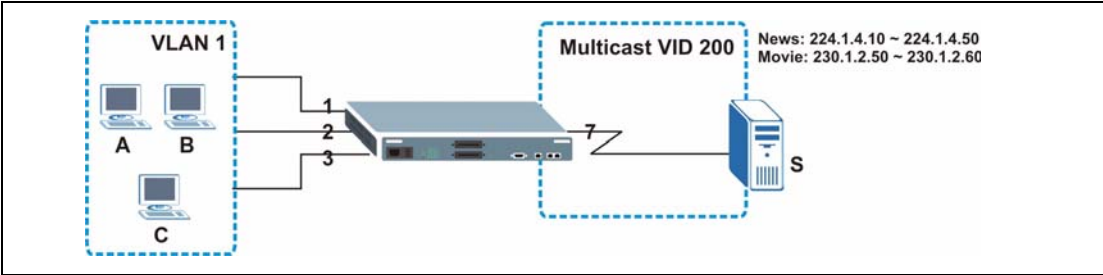
To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 73   MVR Configuration Example

To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 74   MVR Group Configuration Example

Figure 75   MVR Group Configuration Example

PART IV
IP Application

165

Static Route

This chapter shows you how to configure static routes.

23.1 Configuring Static Routing

Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown.

Figure 76   Static Routing

The following table describes the related labels you use to create a static route.

Table 56   Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.

Table 56 Static Routing (continued)

LABEL	DESCRIPTION
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the above fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

24

RIP

This chapter shows you how to configure RIP (Routing Information Protocol).

24.1 RIP Overview

RIP (Routing Information Protocol allows a routing device to exchange routing information with other routers. The **Direction** field controls the sending and receiving of RIP packets. When set to:

* **Both** - the Switch will broadcast its routing table periodically and incorporate the RIP information that it receives.
* **Incoming** - the Switch will not send any RIP packets but will accept all RIP packets received.
* **Outgoing** - the Switch will send out RIP packets but will not accept any RIP packets received.
* **None** - the Switch will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Switch sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

24.2 Configuring RIP

Click **IP Application** > **RIP** in the navigation panel to display the screen as shown. You cannot manually configure a new entry. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to Section 7.6 on page 78).

Figure 77 RIP

The following table describes the labels in this screen.

Table 57 RIP

LABEL	DESCRIPTION
Active	Select this check box to enable RIP on the Switch.
Index	This field displays the index number of an IP interface.
Network	This field displays the IP interface configured on the Switch. Refer to the section on IP Setup for more information on configuring IP domains.
Direction	Select the RIP direction from the drop-down list box. Choices are **Outgoing**, **Incoming**, **Both** and **None**.
Version	Select the RIP version from the drop-down list box. Choices are **RIP-1**, **RIP-2B** and **RIP-2M**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.

IGMP

This chapter shows you how to configure IGMP.

25.1 IGMP Overview

IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

The Switch supports IGMP version 1 (**IGMP-v1**), version 2 (**IGMP-v2**) and version 3 (IGMP-v3). At start up, the Switch queries all directly connected networks to gather group membership. After that, the Switch periodically updates this information.

25.2 Configuring IGMP

Click **IP Application** > **IGMP** in the navigation panel to display the screen as shown next. Each entry in the table is automatically created when you configure a new IP domain in the **IP Setup** screen (refer to Section 7.6 on page 78).

Figure 78   IGMP

The following table describes the labels in this screen.

Table 58   IGMP

LABEL	DESCRIPTION
Active	Select this check box to enable IGMP on the Switch. Note: You *cannot* enable both IGMP snooping and IGMP at the same time. Refer to the section on IGMP snooping.
Index	This field displays an index number of an entry.
Network	This field displays the IP domain configured on the Switch. Refer to Section 7.6 on page 78 for more information on configuring IP domains.
Version	Select an IGMP version from the drop-down list box. Choices are **IGMP-v1**, **IGMP-v2**, **IGMP-v3** and **None**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

26.1 DiffServ Overview

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

26.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 79   DiffServ: Differentiated Service Field
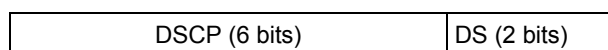
DSCP (6 bits)	DS (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

26.1.2 DiffServ Network Example

The following figure depicts a simple DiffServ network consisting of a group of contiguous DiffServ-compliant network devices.

Figure 80 DiffServ Network Example
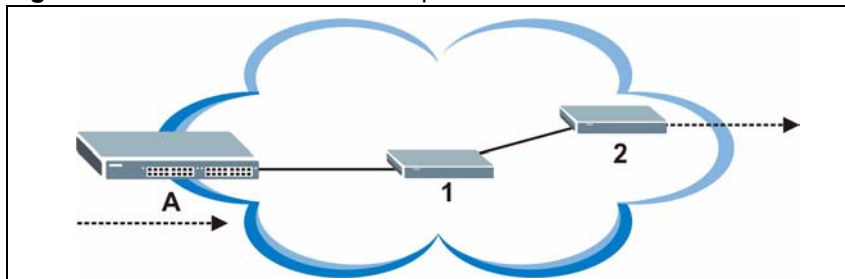
Switch **A** marks traffic flowing into the network based on the configured marking rules. Intermediary network devices **1** and **2** allocate network resources (such as bandwidth) by mapping the DSCP values and the associated policies.

26.2 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 81 DiffServ

The following table describes the labels in this screen.

Table 59 DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the Switch.

Table 59 DiffServ (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select **Active** to enable DiffServ on the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

26.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

Table 60 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

26.3.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping, click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 82   DSCP Setting

The following table describes the labels in this screen.

Table 61 DSCP Setting

LABEL	DESCRIPTION
0 … 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

DHCP

This chapter shows you how to configure the DHCP feature.

27.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the Switch as a DHCP server or disable it. When configured as a server, the Switch provides the TCP/IP configuration for the clients. If you disable the DHCP service, you must have another DHCP server on your LAN, or else the computer must be manually configured.

27.1.1 DHCP modes

The Switch can be configured as a DHCP server or DHCP relay agent.

 • If you configure the Switch as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers.
 • If there is an Ethernet device that performs the DHCP server function for your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the Ethernet device (the DHCP server) for the necessary IP information, and then relays the assigned information back to the computer.

27.2 DHCP Server Status

Click **IP Application** > **DHCP** in the navigation panel. The **DHCP Server Status** screen displays.

Figure 83   DHCP Server Status

The following table describes the labels in this screen.

Table 62   DHCP Server Status

LABEL	DESCRIPTION
Index	This is the index number.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Server Status	This field displays the starting DHCP client IP address.
IP Pool Size	This field displays the size of the DHCP client IP address pool.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to end status polling.

27.3 Configuring DHCP Server

Use this screen to configure your DHCP server settings. Click **IP Application** > **DHCP > Server** to display the **DHCP Server Status** screen.

Figure 84   DHCP Server

The following table describes the labels in this screen.

Table 63   DHCP Server

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN group to which this DHCP settings apply.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool.
IP Subnet Mask	Enter the subnet mask for the client IP pool.
Default Gateway	Enter the IP address of the default gateway device.
Primary/ Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configurations.
Clear	Click **Clear** to reset the fields back to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays **Server** for the DHCP mode.
DHCP Status	This field displays the starting and the size of DHCP client IP address.

Table 63   DHCP Server (continued)

LABEL	DESCRIPTION
Delete	Click **Delete** to remove the selected entry.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

27.3.1 DHCP Server Configuration Example

The follow figure shows a network example where the Switch is used to assign network information to the DHCP clients in the **RD** and **Sales** network.

Figure 85   DHCP Server Network Example
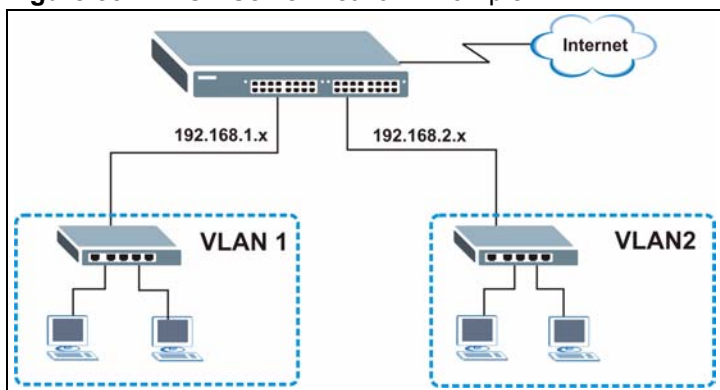
In the **DHCP Server** screen, configure two DHCP client IP address pools for the two networks. The following shows an example.

Figure 86   DHCP Server Configuration Example

27.4 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same subnet. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

27.4.1 DHCP Relay Agent Information

The Switch can add information to client DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the Switch to add to the client DHCP requests that it relays to the DHCP server. Please refer to RFC 3046 for more details.

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server. The following lists the DHCP relay agent option 82 information that the Switch sends to the DHCP server:

- Slot ID (1 byte)
- Port ID (1 byte)
- VLAN ID (2 bytes)
- System name (up to 32 bytes, this is optional)

27.4.2 Configuring DHCP Relay

Configure DHCP relay in the **DHCP Relay** screen. Click **IP Application** > **DHCP** > **Relay** to display the screen as shown.

Figure 87   DHCP Relay

The following table describes the labels in this screen.

Table 64 DHCP Relay

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to discard all changes and start configuring the screen again.
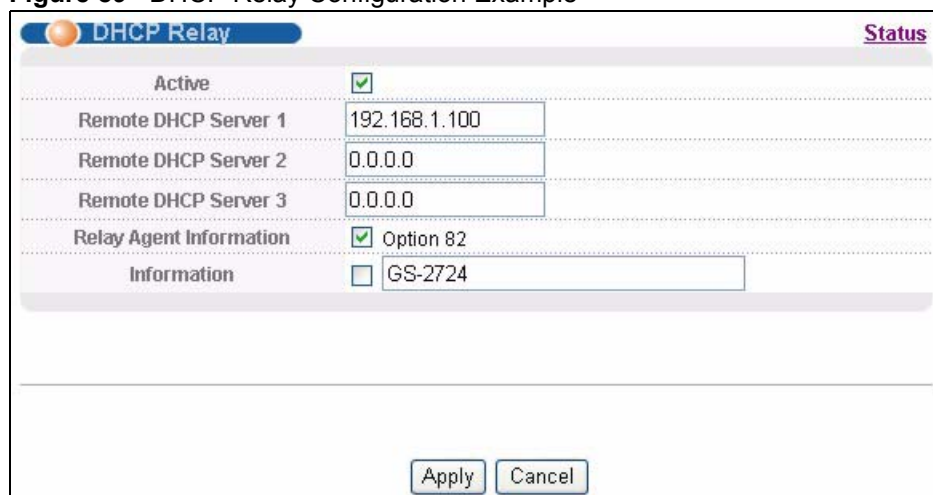
27.4.3 DHCP Relay Configuration Example

The follow figure shows a network example where the Switch is used to relay DHCP requests for the **RD** and **Sales** network. There is only one DHCP server that services the DHCP clients in both networks.

Figure 88   DHCP Relay Network Example
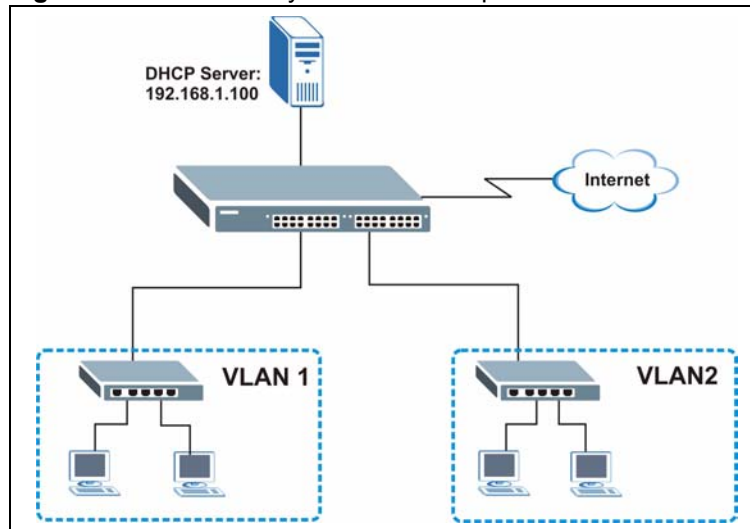
Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 89 DHCP Relay Configuration Example

PART V
Management

Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

28.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 90   Maintenance
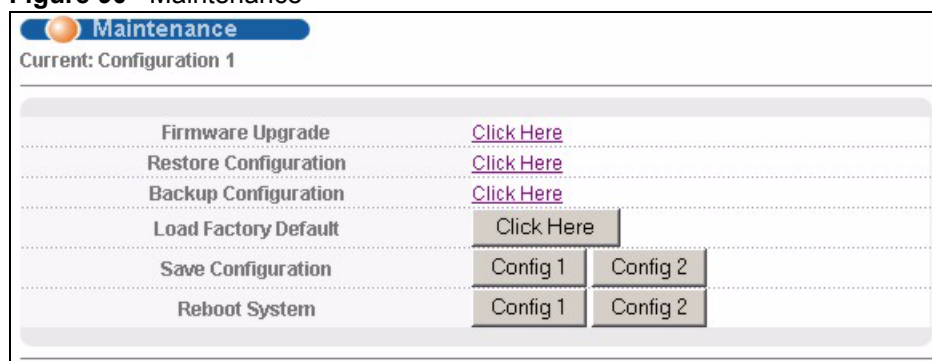
The following table describes the labels in this screen.

Table 65   Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating on the Switch.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Load Factory Default	Click **Click Here** to reset the configuration to the factory default settings.

Table 65   Maintenance (continued)

LABEL	DESCRIPTION
Save Configuratio n	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch. Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the Switch. Click **Config 2** to reboot the system and load **Configuration 2** on the Switch. Note: Make sure to click the **Save** button in any screen to save your settings to the current configuration on the Switch.

28.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

> Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

Figure 91   Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

28.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 92 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

28.4 Backup a Configuration File

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 93 Backup Configuration

Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Click **Backup**.
2 Click **Save** to display the **Save As** screen.
3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

28.5 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults.

2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 94 Load Factory Default
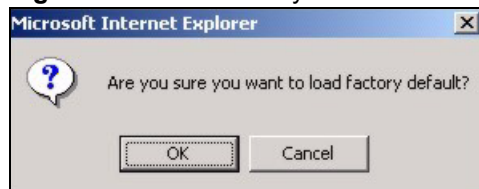
3 In the web configurator, click the **Save** button to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the Switch's default IP address (192.168.1.1).

28.6 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.

Alternatively, click Save on the top right-hand corner in any screen to save the configuration changes to the current configuration.

> Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

28.7 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 95 Reboot System
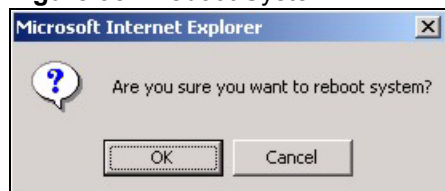
2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

28.8 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

28.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, switch setup, IP Setup, etc. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 66   Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config		This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

28.8.1.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

> Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

28.8.2 FTP Command Line Procedure

1 Launch the FTP client on your computer.
2 Enter `open`, followed by a space and the IP address of your Switch.
3 Press [ENTER] when prompted for a username.
4 Enter your password as requested (the default is "1234").

5 Enter `bin` to set transfer mode to binary.

6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See Table 66 on page 191 for more information on filename conventions.

7 Enter `quit` to exit the ftp prompt.

28.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

28.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the Telnet session immediately.

Access Control

This chapter describes how to control access to the Switch.

29.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share four sessions, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 67   Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to four sessions	One session	Up to five accounts	No limit	

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See Section 38.11.2 on page 237 for more information on disabling multi-login.

29.2 The Access Control Main Screen

Click **Management** > **Access Control** in the navigation panel to display the main screen as shown.

Figure 96   Access Control

29.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 97   SNMP Management Model
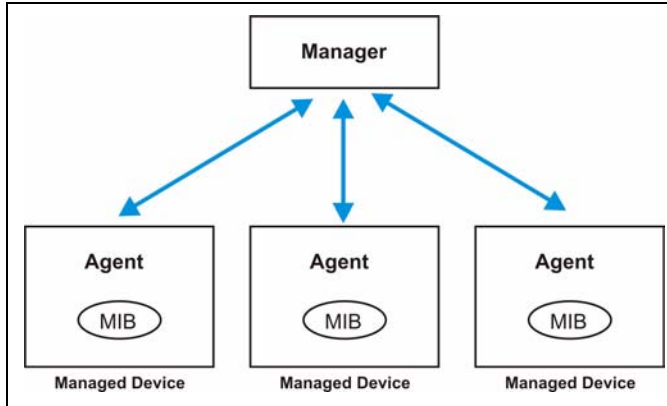
An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the Switch). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 68   SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

29.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

29.3.2 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 69   SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Traps		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP topology changes.
topology change	1.3.6.1.2.1.17.0.2	This trap is sent when the STP root switch changes.

29.3.3 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 98 SNMP

The following table describes the labels in this screen.

Table 70 SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext-requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

29.3.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

- An administrator is someone who can both view and configure changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure settings.

From the **Access Control** screen, display the **Logins** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 99   Logins

The following table describes the labels in this screen.

Table 71   Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see Chapter 38 on page 229.	
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

29.4 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication

between two hosts over an unsecured network.

Figure 100   SSH Communication Example

29.5 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 101   How SSH Works
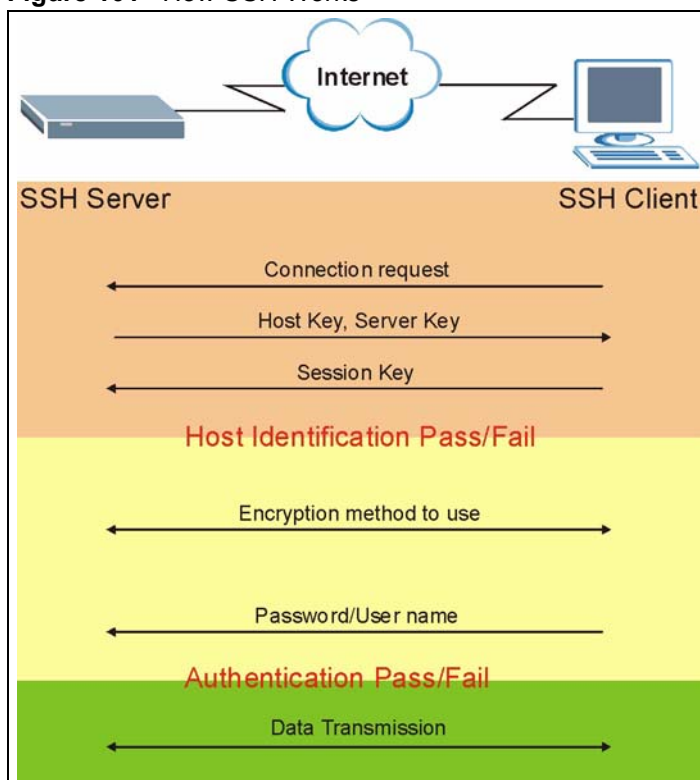
1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrpts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

29.6 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

29.6.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

29.7 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the Switch.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 102 HTTPS Implementation
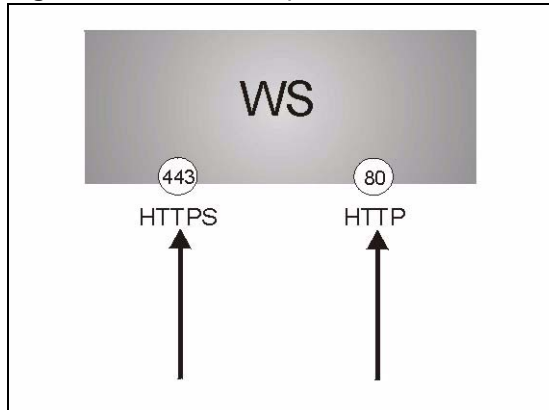
✎ If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

29.8 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

29.8.1 Internet Explorer Warning Messages

When you attempt to access the Switch's HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the Switch.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 103 Security Alert Dialog Box (Internet Explorer)
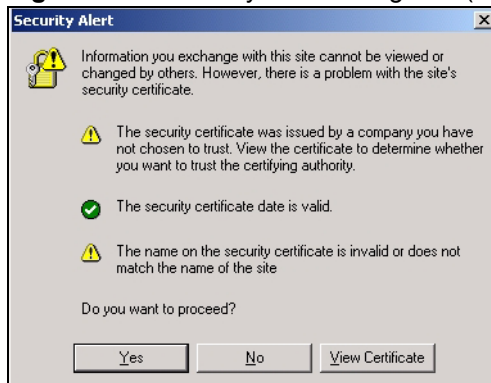
29.8.2 Netscape Navigator Warning Messages

When you attempt to access the Switch's HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the Switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the Switch's certificate into the SSL client.

Figure 104 Security Certificate 1 (Netscape)
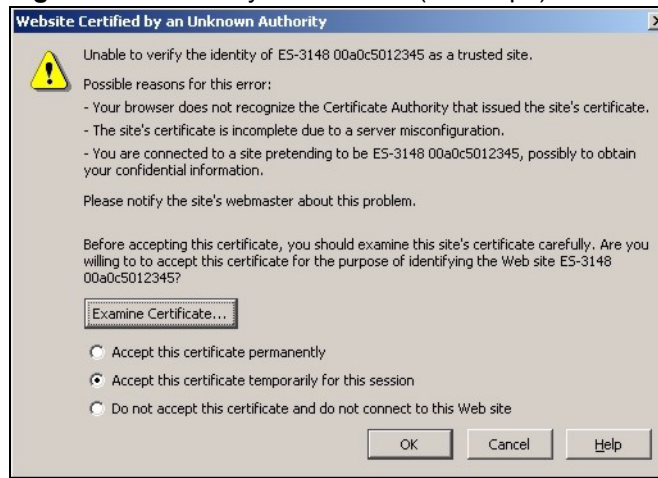
Figure 105 Security Certificate 2 (Netscape)

29.8.3 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 106 Example: Lock Denoting a Secure Connection
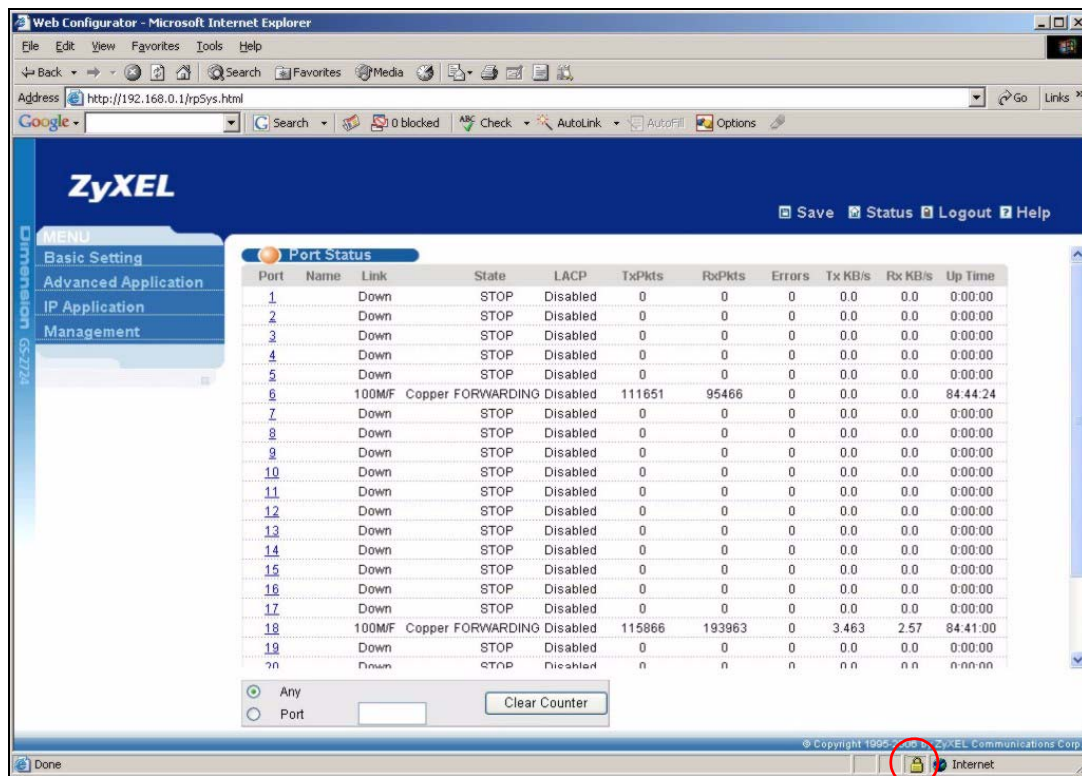
29.9 Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later).

From the **Access Control** screen, display the **Service Access Control** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 107 Service Access Control

The following table describes the fields in this screen.

Table 72 Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

29.10 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 108 Remote Management

The following table describes the labels in this screen.

Table 73 Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.

Table 73 Remote Management (continued)

LABEL	DESCRIPTION
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

Diagnostic

This chapter explains the **Diagnostic** screen.

30.1 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 109   Diagnostic

The following table describes the labels in this screen.

Table 74   Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.

Table 74   Diagnostic (continued)

LABEL	DESCRIPTION
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.

Syslog

This chapter explains the syslog screens.

31.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 75   Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

31.2 Syslog Setup

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 110 Syslog Setup

The following table describes the labels in this screen.

Table 76 Syslog Setup

LABEL	DESCRIPTION
Syslog	Select **Active** to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

31.3 Syslog Server Setup

Click **Management** > **Syslog** > **Syslog Server Setup** to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 111 Syslog Server Setup

The following table describes the labels in this screen.

Table 77 Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to reset the fields.

Cluster Management

This chapter introduces cluster management.

32.1 Cluster Management Status Overview

Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 78   ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 112   Clustering Application Example
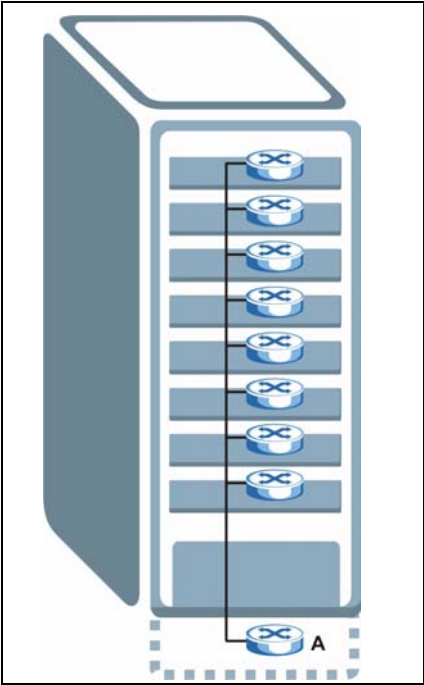
32.2 Cluster Management Status

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

✏️ A cluster can only have one manager.

Figure 113   Cluster Management Status

The following table describes the labels in this screen.

Table 79 Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see Figure 114 on page 213).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member switch is accessible) **Error** (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

32.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 114   Cluster Management: Cluster Member Web Configurator Screen
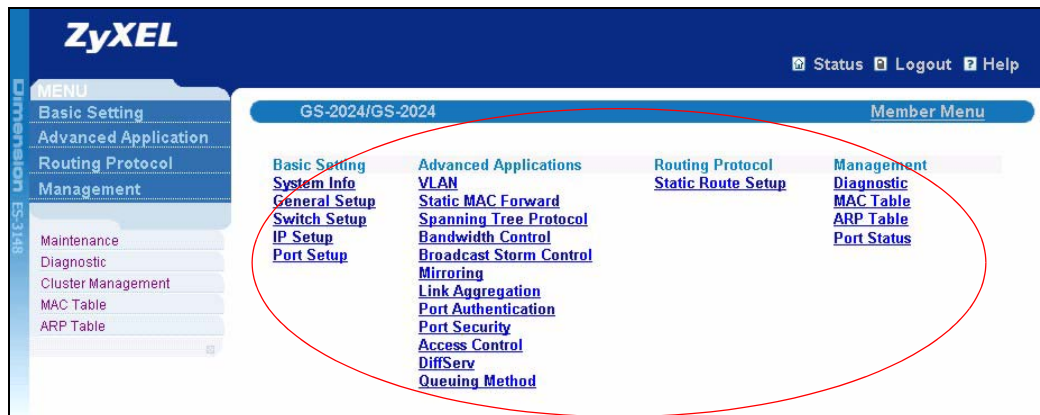
32.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 115   Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-  1 owner    group          393216 Jul 01 12:00 config
--w--w--w-  1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-  1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 370lt0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 80   FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
`User`	Enter "admin".
`Password`	The web configurator password default is 1234.
`ls`	Enter this command to list the name of cluster member switch's firmware and configuration file.
`360lt0.bin`	This is the name of the firmware file you want to upload to the cluster member switch.
`fw-00-a0-c5-01-23-46`	This is the cluster member switch's firmware name as seen in the cluster manager switch.
`config-00-a0-c5-01-23-46`	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

32.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 116 Clustering Management Configuration

The following table describes the labels in this screen.

Table 81 Clustering Management Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.

Table 81 Clustering Management Configuration (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to reset the fields.

MAC Table

This chapter introduces the **MAC Table** screen.

33.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the MAC table to determine how to forward frames. See the following figure.

1 The Switch examines a received frame and learns the port on which this source MAC address came.
2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.

 • If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
 • If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
 • If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.
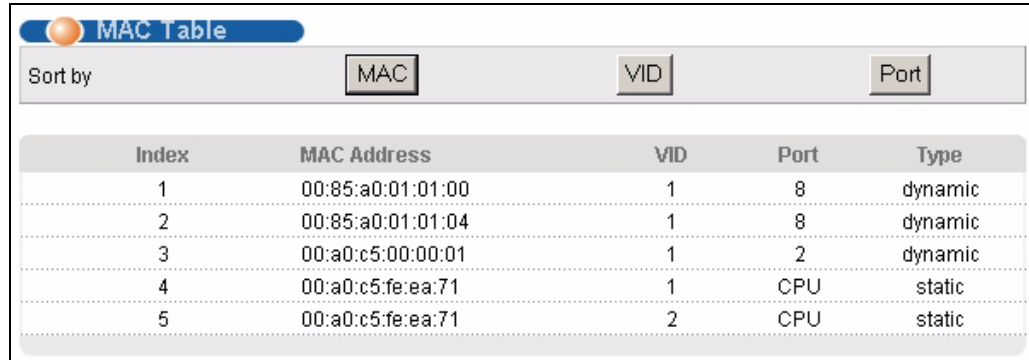
Figure 117   MAC Table Flowchart
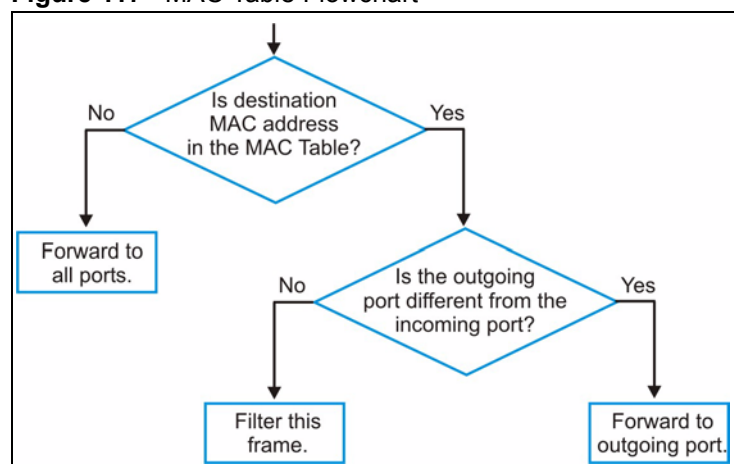
33.2 Viewing the MAC Table

Click **Management** > **MAC Table** in the navigation panel to display the following screen.

Figure 118   MAC Table

The following table describes the labels in this screen.

Table 82   MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

34

IP Table

This chapter introduces the IP table.

34.1 IP Table Overview

The **IP Table** screen shows how packets are forwarded or filtered across the Switch's ports. It shows what device IP address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

The Switch uses the IP table to determine how to forward packets. See the following figure.

1 The Switch examines a received packet and learns the port on which this source IP address came.

2 The Switch checks to see if the packet's destination IP address matches a source IP address already learned in the IP table.

• If the Switch has already learned the port for this IP address, then it forwards the packet to that port.

• If the Switch has not already learned the port for this IP address, then the packet is flooded to all ports. Too much port flooding leads to network congestion.

• If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.
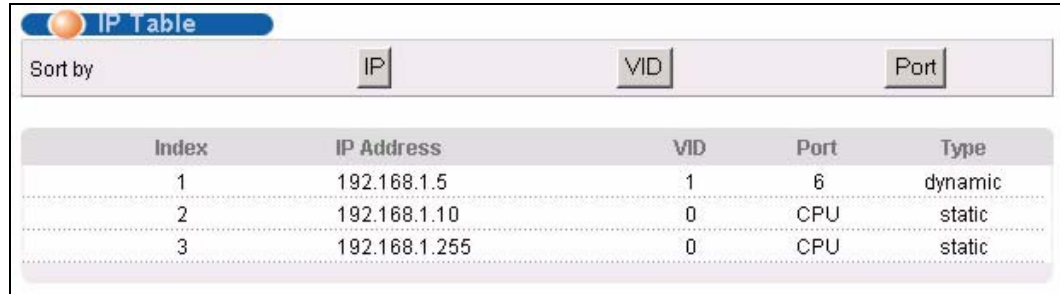
Figure 119   IP Table Flowchart
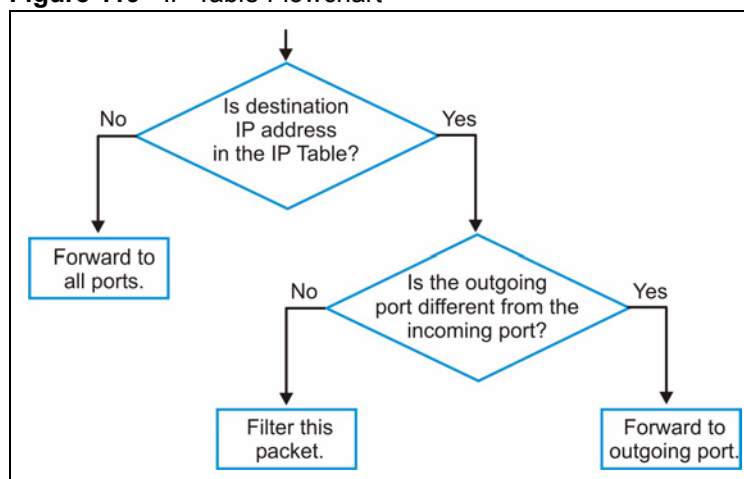
34.2 Viewing the IP Table

Click **Management** > **IP Table** in the navigation panel to display the following screen.

Figure 120   IP Table

The following table describes the labels in this screen.

Table 83   IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays **CPU** to indicate the IP address belongs to the Switch.
Type	This shows whether the IP address is **dynamic** (learned by the Switch) or **static** (belonging to the Switch).

35

ARP Table

This chapter introduces ARP Table.

35.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

35.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

35.2 Viewing the ARP Table

Click **Management** > **ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

Figure 121 ARP Table

The following table describes the labels in this screen.

Table 84 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a Switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

Routing Table

This chapter introduces the routing table.
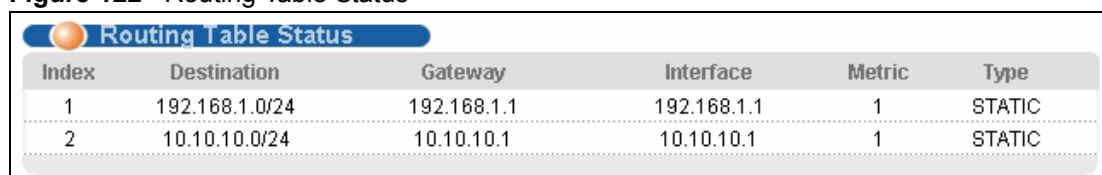
36.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach. The Switch automatically updates the routing table with the RIP information received from other Ethernet devices.

36.2 Viewing the Routing Table

Use this screen to view routing table information. Click **Management** > **Routing Table** in the navigation panel to display the screen as shown.

Figure 122   Routing Table Status

The following table describes the labels in this screen.

Table 85   Routing Table Status

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route.

Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

37.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management** > **Configure Clone** to open the following screen.

Figure 123   Configure Clone

The following table describes the labels in this screen.

Table 86   Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied.
	Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash.
	Example:
	• **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports.
	• **2-6** indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (you configured in the **Basic Setting** menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the **Advanced Application** menus) should be copied to the destination ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

PART VI

CLI and Troubleshooting

227

38

Introducing Commands

This chapter introduces commands and gives a summary of commands available.

38.1 Overview

In addition to the web configurator, you can use commands to configure the Switch. Use commands for advanced diagnosis and troubleshooting. If you have problems with your Switch, customer support may request that you issue some of these commands to assist them in troubleshooting.

✎ See the web configurator parts of this User's Guide for background information on features configurable by the web configurator.

38.2 Accessing the CLI

You can use a direct console connection or Telnet to access the command interpreter on the Switch.

✎ The Switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

- By default, multiple command interpreter management session are allowed via either the console port or Telnet. However, no more than five concurrent login sessions are allowed.

- Use the `configure multi-login` command in the configuration mode to limit concurrent logins to one. Console port access has higher priority.

38.2.1 The Console Port

Connect to the Switch's console port using a terminal emulation software configured to the following settings:

- VT100 terminal emulation
- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control

38.2.1.1 Initial Screen

When you turn on your Switch, it performs several internal tests as well as line initialization. You can view the initialization information using the console port. After the initialization, the login screen displays (refer to).

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:13:49:00:00:01
initialize switch, ethernet address: 00:13:49:00:00:02
Initializing switch unit 0...
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Press ENTER to continue...
```

Use the following steps to Telnet into your Switch.

1 For local management, connect your computer to the RJ-45 management port (labeled **MGMT**) on the Switch.

2 Make sure your computer IP address and the Switch's IP address are on the same subnet. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type `telnet 192.168.0.1` (the default management IP address) and click **OK**.

3 A login screen displays (refer to).

38.3 The Login Screen

After you have successfully established a connection to the Switch using a direct console connection or Telnet, a login screen displays as shown below. For your first login, enter the default administrator login username "admin" and password "1234".

```
                     Enter User Name : admin
                     Enter Password : XXXX
```

38.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in `courier new font`.

- The required fields in a command are enclosed in angle brackets <>, for instance, `ping <ip>` means that you must specify an IP number for this command.
- The optional fields in a command are enclosed in square brackets [], for instance,

`configure snmp-server [contact <system contact>] [location <system location>]`

means that the contact and location fields are optional.
- "Command" refers to a command used in the command line interface (CI command).
- The | symbol means "or".
- The entry <cr> in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up or down arrow key to scroll through the command history list.
- You may enter a unique part of a command and press [TAB] to have the Switch automatically display the full command. For example, if you enter "`config`" and press [TAB], the full command of "`configure`" automatically displays.
- Each interface refers to an Ethernet port on the Switch. Commands configured after the interface command correspond to those ports.
- Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

38.5 Changing the Password

This command is used to change the password for Enable mode. By default the same password is used to enter the command line interface (CLI) and Enable and Config modes of the CLI.

The password you change with this command is required to enter Enable and Config modes of the CLI.

Syntax:

`password <password>`

where

`password <password>`	=	Specifies the new password (up to 32 alphanumeric characters) users have to type in to enter Enable and Config modes.

38.6 Privilege Levels

You can use a command whose privilege level is equal to or less than that of your login account. For example, if your login account has a privilege level of 12, you can use all commands with privilege levels from 0 to 12. 0 privilege level commands are available to all login accounts.

✎ If you use an external RADIUS server to authenticate users, you can use a VSA (Vendor Specific Attribute) to configure a privilege level for an account on the RADIUS server. See Section 16.1.1.1 on page 121 for more information.

Use the following commands to specify privilege levels for login accounts.

Syntax:

```
logins username <username> password <password>
logins username <username> privilege <0-14>
```

where

`username <username>`	=	Specifies a new user (up to 32 alphanumeric characters). Enter a user name to change the settings of an existing account.
`password <password>`	=	Specifies the new password (up to 32 alphanumeric characters) for this user.
`privilege <0-14>`	=	Assigns a privilege level for the user.

38.7 Command Modes

There are three command modes: **User**, **Enable** and **Configure**. The modes (and commands) available to you depend on what level of privilege your account has. See for more information on setting up privilege levels.

When you first log into the command interpreter with a read-only account (having a privilege of 0 to 12), the initial mode is the User mode. The User mode commands are a subset of Enable mode commands. The User mode command prompt ends with an angle bracket (>).

To enter Enable mode, type `enable` and enter the administrator password when prompted (the default is 1234). When you enter Enable mode, the command prompt changes to the pound sign (#). If you log into the command interpreter as an administrator you automatically enter Enable mode.

The following table describes command interpreter modes and how to access them.

Table 87 Command Interpreter Mode Summary

MODE	.DESCRIPTION	HOW TO LOGIN/ACCESS	PROMPT
User	Commands available in this mode are a subset of enable mode. You can perform basic tests and display general system information.	Default login level for a read-only account.	`sysname>` The first part of the prompt is the system name. In the CLI examples in this User's Guide, the system name is always "sysname".
Enable	Commands available in this mode allow you to save configuration settings, reset configuration settings as well as display further system information. This mode also contains the `configure` command which takes you to config mode.	Default login level for accounts with a privilege of 13 or 14. Read-only accounts (with a privilege of 0-12) need to type the `enable` command and enter enable mode password.	`sysname#`
Config	Commands available in this mode allow you to configure settings that affect the Switch globally.	Type `config` in enable mode.	`sysname(config)#`

Table 87 Command Interpreter Mode Summary (continued)

MODE	.DESCRIPTION	HOW TO LOGIN/ ACCESS	PROMPT
Command modes that follow are sub-modes of the config mode and can only be accessed from within the config mode.			
Config-vlan	This is a sub-mode of the config mode and allows you to configure VLAN settings.	Type `vlan` followed by a number (between 1 to 4094). For example, `vlan 10` to configure settings for VLAN 10.	`sysname(config-vlan)#`
Config-interface	This is a sub-mode of the config mode and allows you to configure port related settings.	Type `interface port-channel` followed by a port number. For example, `interface port-channel 8` to configure port 8 on the Switch.	`sysname(config-interface)#`
Config-mvr	This is a sub-mode of the config mode and allows you to configure multicast VLAN settings.	To enter `MVR` mode, enter `mvr` followed by a VLAN ID (between 1 and 4094). For example, enter `mvr 2` to configure multicast settings on VLAN 2.	`sysname(config-mvr)#`

Enter `exit` to quit from the current mode or enter `logout` to exit the command interpreter.

38.8 Getting Help

The system includes a help facility to provide you with the following information about the commands:

- List of available commands under a command group.
- Detailed descriptions of the commands.

38.8.1 List of Available Commands

Enter "help" to display a list of available commands and the corresponding sub commands.

```
sysname> help
  Commands available:

  help
  logout
  exit
  history
  enable
  show ip <cr>
  show hardware-monitor <C|F>
  show system-information
  ping <ip|host-name> <cr>
  ping <ip|host-name> [vlan <vlan-id>][..]
  ping help
  traceroute <ip|host-name> <cr>
  traceroute <ip|host-name> [vlan <vlan-id>][..]
  traceroute help
  ssh <1|2> <[user@]dest-ip> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
sysname>
```

Enter "?" to display a list of commands you can use.

```
sysname> ?
    enable                  Turn on privileged commands
    exit                    Exit from the EXEC
    help                    Description of the interactive help system
    history                 Show a list of previously run commands
    logout                  Exit from the EXEC
    ping                    Exec ping
    show                    Show system information
    ssh                     SSH client
    traceroute              Exec traceroute
sysname>
```

Enter <command> help to display detailed sub commands and parameters.

```
sysname> ping help
  Commands available:

  ping <ip|host-name>
    <
      [ in-band|out-of-band|vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
sysname>
```

Enter <command> ? to display detailed help information about the sub commands and parameters.

```
sysname> ping ?
    <ip|host-name>            destination ip address
    help                      Description of ping help

sysname>
```

38.9 Using Command History

The Switch keeps a list of recently used commands available to you for reuse. You can use any commands in the history again by pressing the up (▲) or down (▼) arrow key to scroll through the previously used commands and press [ENTER]. Use the history command to display the list of commands.

```
sysname> history
  enable
  exit
  show ip
  history
sysname>
```

38.10 Saving Your Configuration

After you set the Switch's settings with the configuration commands, use the write memory command to save the changes permanently.

✎ The write memory command is not available in User mode.

✎ You must save your changes after each CLI session. All unsaved configuration changes are lost once you restart the Switch.

```
sysname# write memory
```

38.10.1 Configuration File

When you configure the Switch using either the CLI (Command Line Interface) or web configurator, the settings are saved as a series of commands in a configuration file on the Switch. You can perform the following with a configuration file:

- Back up configuration once the Switch is set up to work in your network.
- Restore configuration.
- Use the same configuration file to set all Switches (of the same model) in your network to the same settings.

You may also edit a configuration file using a text editor.

Make sure you use valid commands. The Switch rejects configuration files with invalid or incomplete commands.

38.10.2 Logging Out

In User or Enable mode, enter the `exit` or `logout` command to log out of the CLI. In Config mode entering `exit` takes you out of the Config mode and into Enable mode and entering `logout` logs you out of the CLI.

38.11 Command Summary

The following sections summarize the commands available in the Switch together with a brief description of each command. Commands listed in the tables are in the same order as they are displayed in the CLI. See the related section in the User's Guide for more background information.

38.11.1 User Mode

The following table describes the commands available for User mode.

Table 88 Command Summary: User Mode

COMMAND		DESCRIPTION	PRIVILEGE
`help`		Displays help information.	0
`logout`		Exits from the CLI.	0
`exit`		Logs out from the CLI.	0
`history`		Displays a list of previously command(s) that you have executed. The Switch stores up to 256 commands in history.	0

Table 88 Command Summary: User Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
enable		Accesses Enable (or privileged) mode. See Section 38.11.2 on page 237.	0
show	ip	Displays IP related information.	0
	hardware-monitor <C|F>	Displays current hardware monitor information with the specified temperature unit (Celsius **C** or Fahrenheit **F**).	0
	system-information	Displays general system information.	0
ping	<IP|host-name>	Sends Ping request to an Ethernet device.	0
	<IP|host-name> [vlan <vlan-id>] [size <0-1472>] [-t]	Sends Ping request to an Ethernet device in the specified VLAN(s) with the specified parameters.	0
	help	Displays command help information.	0
traceroute	<ip|host-name>	Determines the path a packet takes to a device.	0
	<ip|host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to a device in a VLAN.	0
	help	Displays command help information.	0
ssh	<1|2> <[user@]dest-ip>	Connects to an SSH server with the specified SSH version.	0

38.11.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 89 Command Summary: Enable Mode

COMMAND			DESCRIPTION	PRIVILEGE
baudrate <1|2|3|4|5>			Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).	13
boot	config <index>		Restarts the system with the specified configuration file.	13
configure			Accesses Configuration mode. See Section 38.11.3 on page 242.	13
copy	running-config tftp <ip> <remote-file>		Backs up running configuration to the specified TFTP server with the specified file name.	13
	running-config interface port-channel <port> <port-list>		Clones (copies) the attributes from the specified port to other ports.	13

Table 89 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`running-config interface port-channel <port> <port-list>`	`[bandwidth-limit ....]`	Copies the specified attributes from one port to other ports.	13
	`tftp`	`config <index> <ip> <remote-file>`	Restores configuration with the specified filename from the specified TFTP server to the specified configuration file on the router.	13
		`flash <ip> <remote-file>`	Restores firmware via TFTP.	13
`disable`			Exits Enable (or privileged) mode.	13
`enable`			Accesses Enable (or privileged) mode.	13
`erase`	`running-config`		Resets to the factory default settings.	13
		`interface port-channel <port-list> [bandwidth-limit...]`	Resets to the factory default settings on a per port basis and optionally on a per feature configuration basis.	13
`exit`			Exits Enable (or privileged) mode.	13
`help`			Displays help information.	13
`history`			Displays a list of command(s) that you have previously executed.	13
`igmp-flush`			Removes all IGMP information.	13
`kick`	`tcp <Session ID>`		Disconnects the specified TCP session.	13
`logout`			Exits Enable (or privileged) mode.	13
`mac-flush`			Clears the MAC address table.	13
	`<port-num>`		Removes all learned MAC address on the specified port(s).	13
`no`	`logging`		Disables syslog logging.	13
`ping <IP|host-name>`			Sends Ping request to an Ethernet device.	13
	`[vlan <vlan-id>][..]`		Sends Ping request to an Ethernet device in the specified VLAN(s).	13
`reload`	`config <index>`		Restarts the system and use the specified configuration file.	13
`show`	`classifier`		Displays all classifier related information.	13
		`[name]`	Displays the specified classifier related information.	13
	`cluster`		Displays cluster management status.	13

Table 89 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`candidates`	Displays cluster candidate information.	13
		`member`	Displays the MAC address of the cluster member(s).	13
		`member config`	Displays the configuration of the cluster member(s).	13
		`member mac <mac-addr>`	Displays the status of the cluster member(s).	13
	`dhcp`	`relay`	Displays DHCP relay settings.	13
		`server`	Displays DHCP server settings.	13
		`server <vlnd-id>`	Displays DHCP server settings in a specified VLAN.	13
	`diffserv`		Displays general DiffServ settings.	13
	`garp`		Displays GARP information.	13
	`hardware-monitor`	`<C|F>`	Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	13
	`https`		Displays the HTTPS information.	13
		`certificate`	Displays the HTTPS certificates.	13
		`key <rsa|dsa>`	Displays the HTTPS key.	13
		`session`	Displays current HTTPS session(s).	13
		`timeout`	Displays the HTTPS session timeout.	13
	`igmp-filtering`	`profile [name]`	Displays IGMP filtering profile settings.	13
	`igmp-snooping`		Displays global IGMP snooping settings.	13
	`interface <port-number>`		Displays current interface status.	13
	`interfaces <port-list>`		Displays current interfaces status.	13
	`interfaces config <port-list>`		Displays current interface configuration.	13
		`bandwidth-control`	Displays bandwidth control settings.	13
		`bstorm-control`	Displays broadcast storm control settings.	13
		`egress`	Displays outgoing port information.	13
		`igmp-filtering`	Displays IGMP filtering settings.	13
		`igmp-group-limited`	Displays the IGMP group limit.	13

Table 89 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`igmp-immediate-leave`	Displays the IGMP Immediate Leave setting.	13
		`igmp-query-mode`	Displays IGMP query mode for the specified port.	13
	`ip`		Displays IP related information.	13
		`arp`	Displays the ARP table.	13
		`igmp`	DIsplays the IGMP setting.	13
		`iptable all [IP|VID|PORT]`	Displays the IP address table. You can sort the table based on the IP address, VLAN ID or the port number.	13
		`iptable count`	Displays the number of IP addresses in the IP table.	13
		`iptable static`	Displays the status IP address table.	13
		`route`	Displays IP routing information.	13
		`route static`	Displays IP static route information.	13
		`tcp`	Displays IP TCP information.	13
		`udp`	Displays IP UDP information.	13
	`lacp`		Displays LACP (Link Aggregation Control Protocol) settings.	13
	`logging`		Displays system logs.	13
	`loginPrecedence`		Displays login precedence settings.	13
	`logins`		Displays login account information.	13
	`mac`	`address-table <all [mac|vid|port]>`	Displays MAC address table. You can sort by MAC address, VID or port.	13
		`address-table static`	Displays static MAC address table.	13
		`address-table count`	Displays the number of entries in the MAC address table.	13
	`mac-aging-time`		Displays MAC learning aging time.	13
	`mac-count`		Displays the count of MAC addresses learnt.	13
	`mrstp <tree-index>`		Displays multiple rapid spanning tree configuration for the specified tree.	13
	`multicast`		Displays multicast settings.	13
	`multi-login`		Displays multi-login information	14
	`mvr`		DIsplays all MVR settings.	13

Table 89 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`<VID>`	Displays the specified MVR group settings.	13
	`policy`		Displays all policy related information.	13
		`[name]`	Displays the specified policy related information.	13
	`port-access-authenticator`		Displays all port authentication settings.	13
		`[port-list]`	Displays port authentication settings on the specified port(s).	13
	`port-security`		Displays all port security settings.	13
		`[port-list]`	Displays port security settings on the specified port(s).	13
	`radius-server`		Displays RADIUS server settings.	13
	`remote-management`		Displays all secured client information.	13
		`[index]`	Displays the specified secured client information.	13
	`router`	`igmp`	Displays global IGMP settings.	13
		`rip`	Displays global RIP settings.	13
	`running-config`		Displays current operating configuration.	13
		`interface port-channel <port-list> [bandwidth-limit...]`	Displays current operating configuration on a port by port basis. Optionally specifies which settings are displayed.	13
	`service-control`		Displays service control settings.	13
	`snmp-server`		Displays SNMP settings.	13
	`spanning-tree`	`config`	Displays Spanning Tree Protocol (STP) settings.	13
	`ssh`		Displays general SSH settings.	13
		`known-hosts`	Displays known SSH hosts information.	13
		`key <rsa1|rsa|dsa>`	Displays internal SSH public and private key information.	13
		`session`	Displays current SSH session(s).	13
	`system-information`		Displays general system information.	13
	`time`		Displays current system time and date.	13
	`timesync`		Displays time server information.	13
	`trunk`		Displays link aggregation information.	13
	`vlan`		Displays the status of all VLANs.	13

Table 89 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`<vlan-id>`	Displays the status of the specified VLAN.	13
	`vlan-stacking`		Displays VLAN stacking settings.	13
	`vlan1q`	`gvrp`	Displays GVRP settings.	13
		`port-isolation`	Displays port isolation settings.	13
`ssh`	`<1|2> <[user@]dest-ip>`		Connects to an SSH server with the specified SSH version.	13
		`[command </>]`	Connects to an SSH server with the specified SSH version and addition commands to be executed on the server.	13
`traceroute`	`<ip|host-name> [in-band|out-of-band|vlan <vlan-id>][ttl <1-255>] [wait <1-60>] [queries <1-10>]`		Determines the path a packet takes to a device.	13
	`help`		Displays help information for this command.	13
`write`	`memory`		Saves current configuration to the configuration file the Switch is currently using.	13
		`<index>`	Saves current configuration to the specified configuration file on the Switch.	13

38.11.3 General Configuration Mode

The following table lists the commands in Configuration (or Config) mode.

Table 90 Command Summary: Configuration Mode

COMMAND			DESCRIPTION	PRIVILEGE
`admin-password`	`<pw-string> <confirm-string>`		Changes the administrator password.	14
`bandwidth-control`			Enables bandwidth control.	13
`bcp-transparency`			Enables Bridge Control Protocol (BCP) transparency.	13

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
classifier	`<name> <[packet-format <802.3untag|802.3tag| EtherIIuntag| EtherIItag>] [priority <0-7>] [vlan <vlan-id>][ethernet-type <ether-num|ip|ipx| arp|rarp| appletalk|decnet| sna|netbios|dlc>] [source-mac <src-mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [dscp <0-63>] [ip-protocol <protocol-num|tcp|udp|icmp|egp|rsvp|igmp| igp|pim|ipsec> [establish-only]] [source-ip <src-ip-addr> [mask-bits <mask-bits>]] [source-socket <socket-num>] [destination-ip <dest-ip-addr> [mask-bits <mask-bits>]] [destination-socket <socket-num>] [inactive]>`		Configures a classifier. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number.	13
	`help`		Displays help information for this command.	13
cluster	`<vlan-id>`		Enables clustering in the specified VLAN group.	13
	`member <mac-address> password <password-str>`		Sets the cluster member.	13
	`name <cluster name>`		Sets a descriptive name for the cluster.	13
	`rcommand <mac-address>`		Logs into the CLI of the specified cluster member.	13
default-management	`<in-band|out-of-band>`		Specifies through which traffic flow the Switch is to send packets.	13
dhcp	`relay`		Enables DHCP relay.	13

243

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`helper-address <remote-dhcp-server1> <remote-dhcp-server2> <remote-dhcp-server3>`	Sets the IP addresses of up to 3 DHCP servers.	13
		`information`	Allows the Switch to add system name to agent information.	13
		`option`	Allows the Switch to add DHCP relay agent information.	13
	`server <vlan-id>`	`starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253> [default-gateway <ip-addr>][primary-dns <ip-addr>] [secondary-dns <ip-addr>]`	Configures a DHCP server for the specified VLAN. Optionally specifies the default gateway and DNS servers for this DHCP server to assign.	13
`diffserv`			Enables DiffServ.	13
	`dscp <0-63> priority <0-7>`		Sets the DSCP-to-IEEE 802.1q mappings.	13
`exit`			Exits from the CLI.	13
`garp`	`join <100-65535> leave <msec> leaveall <msec>`		Configures GARP time settings.	13
`help`			Displays help information.	13
`history`			Displays a list of previous command(s) that you have executed.	13
`hostname`	`<name_string>`		Sets the Switch's name for identification purposes.	13
`https`	`cert-regeneration <rsa|dsa>`		Re-generates a certificate.	13
	`timeout <0-65535>`		Sets the HTTPS timeout period.	13
`igmp-filtering`			Enables IGMP filtering on the Switch.	13
	`profile <name> start-address <ip> end-address <ip>`		Sets the range of multicast address(es) in a profile.	13
`igmp-snooping`			Enables IGMP snooping.	13
	`8021p-priority`	`<0-7>`	Sets the 802.1p priority for outgoing igmp snooping packets.	13

244

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`host-timeout`	`<1-16711450>`	Sets the host timeout value.	13
	`leave-timeout`	`<1-16711450>`	Sets the leave timeout value	13
	`unknown-multicast-frame <drop|flooding>`		Sets how to treat traffic from unknown multicast group.	13
	`reserved-multicast-group <drop|flooding>`		Sets how to treat traffic belonging to reserved multicast groups.	13
`interface`	`port-channel <port-list>`		Enables a port or a list of ports for configuration. See Section 38.11.4 on page 255 for more details.	13
	`route-domain <ip-address>/<mask-bits>`		Enables a routing domain for configuration. See Section 38.11.5 on page 258 for more details.	13
`ip`	`address`	`<ip> <mask>`	Sets the IP address and subnet mask of the out-of-band management port.	13
		`default-gateway <ip>`	Sets the default gateway's IP address for the out-of-band management port.	13
	`name-server`	`<ip>`	Sets the IP address of a domain name server.	13
	`route`	`<ip> <mask> <next-hop-ip>`	Creates a static route.	13
		`<ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]`	Sets the metric of a static route or deactivates a static route.	13
`lacp`			Enables Link Aggregation Control Protocol (LACP).	13
	`system-priority`	`<1-65535>`	Sets the priority of an active port using LACP.	13
`loginPrecedence`	`<LocalOnly | LocalRADIUS | RADIUSOnly>`		Select which database the Switch should use (first) to authenticate a user.	13
`logins`	`username <name> password <pwd>`		Configures up to four read-only login accounts.	14
	`username <name>`	`privilege <0-14>`	Assigns a privilege level to user accounts.	14
`logout`			Exits from the CLI.	13
`mac-aging-time`	`<10-3000>`		Sets learned MAC aging time.	13

245

Table 90   Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
`mac-filter`	`name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>`		Configures a static MAC address port filtering rule.	13
		`inactive`	Disables a static MAC address port filtering rule.	13
`mac-forward`	`name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>`		Configures a static MAC address forwarding rule.	13
		`inactive`	Disables a static MAC address forwarding rule.	13
`mirror-port`			Enables port mirroring.	13
	`<port-num>`		Enables port mirroring on a specified port.	13
`mode`	`zynos`		Changes the CLI mode to the ZyNOS format.	13
`mrstp`	`<tree-index>`		Activates the specified STP configuration.	13
		`priority <0-61440>`	Sets the priority for the specified tree.	13
		`hello-time <1-10> maximum-age <6-40> forward-delay <4-30>`	Sets hello-time, maximum-age and forward delay for the specified tree.	13
	`interface <port-list>`		Activates STP on the specified ports.	13
		`path-cost <1-65535>`	Sets a path cost to the specified ports.	13
		`priority <0-255>`	Sets the priority value to the specified ports for STP.	13
		`tree-index <1-4>`	Assigns a specific STP configuration to the ports.	13
	`help`		Displays the detailed help for the mrstp command.	13
`multi-login`			Enables multi-login.	14
`mvr`	`<vlan-id>`		Enters the MVR (Multicast VLAN Registration) configuration mode. Refer to Section 38.12 on page 260 for more information.	13
`no`	`bandwidth-control`		Disable bandwidth control on the Switch.	13
	`bcp-transparency`			13

Table 90   Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEG E
	`classifier`	`<name>`	Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use policy rule related information.	13
		`<name> inactive`	Enables a classifier.	13
	`cluster`		Disables cluster management on the Switch.	13
		`member <mac-address>`	Removes the cluster member.	13
	`dhcp relay`		Disables DHCP relay.	13
		`information`	Disables the relay agent information option 82.	13
		`option`	System name is not appended to option 82 information field.	13
	`dhcp server <vlan-id>`		Disables DHCP server settings.	13
		`default-gateway`	Disables DHCP server default gateway settings.	13
		`primary-dns`	Disables DHCP primary DNS server settings.	13
		`secondary-dns`	Disables DHCP server secondary DNS settings.	13
	`diffserv`		Disables the DiffServ settings.	13
	`https`	`timeout`	Resets the session timeout to the default of 300 seconds.	13
	`igmp-filtering`		Disables IGMP filtering on the Switch.	13
		`profile <name>`	Disables the specified IGMP filtering profile.	13
		`profile <name> start-address <ip> end-address <ip>`	Clears the settings of the specified IGMP filtering profile.	13
	`igmp-snooping`		Disables IGMP snooping.	13
	`ip`		Sets the management IP address to the default value.	13
		`route <ip> <mask>`	Removes a specified IP static route.	13
		`route <ip> <mask> inactive`	Enables a specified IP static route.	13
	`lacp`		Disables the link aggregation control protocol (dynamic trunking) on the Switch.	13
	`logins <name>`		Disables login access to the specified name.	14

247

Table 90   Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE

	`mac-filter`	`name <name> mac`
		`<mac-addr> vlan`
		`<vlan-id> drop`
		`<src|dst|both>`
		`inactive`
			Enables the specified MAC-filter rule.	13

		`name <name> mac`
		`<mac-addr> vlan`
		`<vlan-id> drop`
		`<src|dst|both>`
			Disables the specified MAC filter rule.	13

	`mac-forward`	`name <name> mac`
		`<mac-addr> vlan`
		`<vlan-id>`
		`interface`
		`<interface-id>`
			Removes the specified MAC forwarding entry, belonging to a VLAN group (if any) forwarded through an interface(s).	13

		`name <name> mac`
		`<mac-addr> vlan`
		`<vlan-id>`
		`interface`
		`<interface-id>`
		`inactive`
			Enables the specified MAC address, belonging to a VLAN group (if any) forwarded through an interface(s).	13

	`mirror-port`		Disables port mirroring on the Switch.	13
	`mrstp`	`<treeIndex>`	Disables the specified STP configuration.	13
	`mrstp`	`interface` `<port-list>`	Disables the STP assignment from the specified port(s).	13
	`multi-login`		Disables another administrator from logging into Telnet or the CLI.	14
	`mvr <vlan-id>`		Disables MVR on the Switch.	13
	`policy <name>`		Deletes the policy. A policy sets actions for the classified traffic.	13
		`inactive`	Enables a policy.	13
	`port-access-` `authenticator`		Disables port authentication on the Switch.	13
		`<port-list>`	Disables authentication on the listed ports.	13
		`<port-list>` `reauthenticate`	Disables the re-authentication mechanism on the listed port(s).	13
	`port-security`		Disables port security on the device.	13
		`<port-list>`	Disables port security on the specified ports.	13
		`<port-list>` `learn inactive`	Enables MAC address learning on the specified ports.	13
	`radius-server`	`<index>`	Disables the use of authentication from the specified RADIUS server.	13

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`remote-management`	`<index>`	Clears a secure client set entry from the list of secure clients.	13
		`<index> service <telnet| ftp| http| icmp| snmp| ssh| https>`	Disables a secure client set entry number from using the selected remote management service.	13
	`router`	`igmp`	Disables IGMP on the Switch.	13
		`rip`	Disable RIP on the Switch.	13
	`service-control`	`ftp`	Disables FTP access to the Switch.	13
		`http`	Disables web browser control to the Switch.	13
		`https`	Disables secure web browser access to the Switch.	13
		`icmp`	Disables ICMP access to the Switch such as pinging and tracerouting.	13
		`snmp`	Disables SNMP management.	13
		`ssh`	Disables SSH (Secure Shell) server access to the Switch.	13
		`telnet`	Disables telnet access to the Switch.	13
	`snmp-server`	`trap-destination <ip>`	Disables sending of SNMP traps to a station.	13
	`spanning-tree`		Disables STP.	13
		`<port-list>`	Disables STP on listed ports.	13
	`ssh`	`key <rsa1|rsa|dsa>`	Disables the secure shell server encryption key. Your Switch supports SSH versions 1 and 2 using RSA and DSA authentication.	13
		`known-hosts <host-ip>`	Removes the specified remote hosts from the list of all known hosts.	13
		`known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]`	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).	13
	`storm-control`		Disables broadcast storm control.	13
	`syslog`		Disables syslog logging.	13
		`server <ip-address>`	Disables syslog logging to the specified syslog server.	13

249

Table 90   Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`server <ip-address> inactive`	Enables syslog logging to the specified syslog server.	13
		`type [type]`	DIsables syslog logging for the specified log type (`sys`, `link`, `config`, `error` or `report`).	13
	`timesync`		Disables timeserver settings.	13
	`trunk`	`<T1|T2|T3|T4|T5 |T6>`	Disables the specified trunk group.	13
		`<T1|T2|T3|T4|T5 |T6> interface <port-list>`	Removes ports from the specified trunk group.	13
		`<T1|T2|T3|T4|T5 |T6> lacp`	Disables LACP in the specified trunk group.	13
	`vlan`	`<vlan-id>`	Deletes the static VLAN entry.	13
	`vlan1q`	`gvrp`	Disables GVRP on the Switch.	13
		`port-isolation`	Disables port isolation.	13
	`vlan-stacking`		Disables VLAN stacking.	13
`password`			Change the password for Enable mode.	14

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
`policy`	`<name> classifier <classifier-list> < [vlan<vlan-id>] [egress-port <port-num>] [priority <0-7>] [dscp <0-63>] [tos <0-7>] [bandwidth <bandwidth>] [outgoing-packet-format <tagged|untagged>] [out-of-profile-dscp <0-63>] [forward-action <drop|forward>] [queue-action <prio-set|prio-queue|prio-replace-tos>] [diffserv-action <diff-set-tos|diff-replace-priority|diff-set-dscp>] [outgoing-mirror] [outgoing-eport] [outgoing-non-unicast-eport] [outgoing-set-vlan] [metering] [out-of-profile-action <[change-dscp][drop][forward] [set-drop-precedence]>] [inactive]>`		Configures a policy. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule ensures that a traffic flow gets the requested treatment in the network.	13
`port-access-authenticator`			Enables 802.1x authentication on the Switch.	13
	`<port-list>`		Enables 802.1x authentication on the specified port(s).	13
		`reauthenticate`	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	13

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`reauth-period <reauth-period>`	Specifies how often a client has to re-enter the username and password to stay connected to the specified port(s).	13
`port-security`			Enables port security on the device.	13
	`<port-list>`		Enables port security on the specified port(s).	13
		`learn inactive`	Disables MAC address learning on the specified port(s).	13
		`address-limit <number>`	Limits the number of (dynamic) MAC addresses that may be learned on a port.	13
		`MAC-freeze`	Adds learned MAC addresses to the static MAC table and stops learning any more MAC addresses.	13
`queue`	`priority <0-7> level <0-7>`		Sets the priority level-to-physical queue mapping.	13
`radius-server`	`host <index> <ip>`		Specifies the IP address of RADIUS server 1 or RADIUS server 2 (index =1 or index =2).	13
		`[auth-port <socket-number>] [key <key-string>]`	Sets the port number and key of the external RADIUS server.	13
	`timeout <1-1000>`		Specifies the RADIUS server timeout value.	13
	`mode`	`<priority|round-robin>`	Specifies the mode for RADIUS server selection.	13
`remote-management`	`<index> start-addr <ip> end-addr <ip> service <telnet|ftp|http|icmp|snmp>`		Specifies a group of trusted computer(s) from which an administrator may use a service to manage the Switch.	13
`router`	`igmp`		Enables and enters the IGMP configuration mode.	13
		`exit`	Leaves the IGMP configuration mode.	13
		`non-querier`	Sets the Switch into a non-querier mode. It will not send igmp query messages.	13
		`no non-querier`	Disables non-querier mode on the Switch.	13
	`rip`		Enables and enters the RIP configuration mode.	13
		`exit`	Leaves the RIP configuration mode.	13

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
service-control	ftp <socket-number>		Allows FTP access on the specified service port.	13
	http <socket-number> <timeout>		Allows HTTP access on the specified service port and defines the timeout period.	13
	https <socket-number>		Allows HTTPS access on the specified service port.	13
	icmp		Allows ICMP management packets.	13
	snmp		Allows SNMP management.	13
	ssh <socket-number>		Allows SSH access on the specified service port.	13
	telnet <socket-number>		Allows Telnet access on the specified service port.	13
snmp-server	[contact <system contact>] [location <system location>]		Sets the geographic location and the name of the person in charge of this Switch.	13
	get-community <property>		Sets the get community.	13
	set-community <property>		Sets the set community.	13
	trap-community <property>		Sets the trap community.	13
	trap-destination <ip>		Sets the IP addresses of up to four stations to send your SNMP traps to.	13
spanning-tree			Enables STP on the Switch.	13
	<port-list>		Enables STP on a specified port.	13
	<port-list> path-cost <1-65535>		Sets the STP path cost for a specified port.	13
	<port-list> priority <0-255>		Sets the priority for a specified port.	13
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.	13
	help		Displays help information.	13
	priority <0-61440>		Sets the bridge priority of the Switch.	13
ssh	known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa> <key>		Adds a remote host to which the Switch can access using SSH service.	13
storm-control			Enables broadcast storm control on the Switch.	13

253

Table 90 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
`syslog`			Enables syslog logging.	13
	`server <ip-address>`	`inactive`	Disables syslog logging to the specified syslog server.	13
		`level [0 ~ 7]`	Sets the IP address of the syslog server and the severity level.	13
	`type <type> facility [local 1 ..7]`		Sets the log type and the file location on the syslog server.	13
`time`	`<Hour:Min:Sec>`		Sets the time in hour, minute and second format.	13
	`date <month/day/ year>`		Sets the date in year, month and day format.	13
	`help`		Displays help information.	13
	`timezone <-1200|...|1200>`		Selects the time difference between UTC (formerly known as GMT) and your time zone.	13
`timesync`	`<daytime|time|ntp>`		Sets the time server protocol.	13
	`server <ip>`		Sets the IP address of your time server.	13
`trunk`	`<T1|T2|T3|T4|T5|T6 >`		Activates a trunk group.	13
	`<T1|T2|T3|T4|T5|T6 >lacp`		Enables LACP for a trunk group.	13
	`<T1|T2|T3|T4|T5|T6 >interface <port-list>`		Adds a port(s) to the specified trunk group.	13
	`interface <port-list> timeout <lacp-timeout>`		Defines the port number and LACP timeout period.	13
`vlan`	`<vlan-id>`		Enters the VLAN configuration mode. See Section 38.11.6 on page 259 for more information.	13
`vlan1q`	`gvrp`		Enables GVRP.	13
	`port-isolation`		Enables port-isolation.	13
`vlan-stacking`			Enables VLAN stacking on the Switch.	13
	`<SPTPID>`		Sets the SP TPID (Service Provider Tag Protocol Identifier).	13
`vlan-type`	`<802.1q|port-based>`		Specifies the VLAN type.	13

38.11.4 interface port-channel Commands

The following table lists the `interface port-channel` commands in configuration mode. Use these commands to configure the ports.

Table 91   interface port-channel Commands

COMMAND			DESCRIPTION	PRIVILEGE
`interface port-channel <port-list>`			Enables a port or a list of ports for configuration.	13
	`bandwidth-limit`		Enables ingress (pir), cir and egress limits on the port(s).	13
		`cir`	Enables the guaranteed bandwidth limits for incoming traffic on the port(s).	13
		`cir <Kbps>`	Sets the guaranteed bandwidth allowed for incoming traffic on the port(s).	13
		`pir`	Enables bandwidth limits allowed for incoming traffic on the port(s).	13
		`pir <Kbps>`	Sets the maximum bandwidth allowed for incoming traffic on the port(s).	13
		`egress`	Enables bandwidth limits allowed for outgoing traffic on the port(s).	13
		`egress <Kbps>`	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).	13
	`bpdu-control <peer|tunnel|discard|network>`		Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states.	13
	`broadcast-limit`		Enables broadcast storm control limit on the port(s).	13
		`<pkt/s>`	Specifies the maximum number of broadcast packets to allow through the port.	13
	`diffserv`		Enables DiffServ on the port(s).	13
	`dlf-limit`		Enables the Destination Lookup Failure (DLF) limit.	13
		`<pkt/s>`	Sets the interface DLF limit in packets per second (pps).	13
	`egress set <port-list>`		Sets the outgoing traffic port list for a port-based VLAN.	13
	`exit`		Exits from the interface port-channel command mode.	13
	`flow-control`		Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	13

Table 91 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
`frame-type <all|tagged|untagged>`			Choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.	13
`ge-spq`	`<q0|q1|...|q7>`		Enables strict priority queuing starting with the specified queue and subsequent higher queues on the Gigabit ports.	13
`gvrp`			Enables this function to permit VLAN groups beyond the local switch.	13
`help`			Displays a description of the interface port-channel commands.	13
`igmp-filtering`	`profile <profile>`		Applies the specified IGMP filtering profile.	13
`igmp-group-limited`			Enables the IGMP group limiting feature.	13
	`number <number>`		Sets the maximum number IGMP groups allowed.	13
`igmp-immediate-leave`			Enables the IGMP immediate leave function.	13
`igmp-querier-mode <auto|fixed|edge>`			Sets the IGMP query mode for the port.	13
`inactive`			Disables the specified port(s) on the Switch.	13
`ingress-check`			Enables the device to discard incoming frames for VLANs that are not included in a port member set.	13
`intrusion-lock`			Enables intrusion lock on the port(s) and a port cannot be connected again after you disconnected the cable.	13
`mirror`			Enables port mirroring in the interface.	13
	`dir <ingress|egress|both>`		Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one or all ports to another or all ports for external analysis.	13
`multicast-limit`			Enables the port(s) multicast limit.	13
	`<pkt/s>`		Sets how many multicast packets the port(s) receives per second.	13
`name <port-name-string>`			Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).	13

256

Table 91 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	no	bandwidth-limit	Disables bandwidth limit on the port(s).	13
		bandwidth-limit <cir>	Disables cir bandwidth limits on the port(s).	13
		bandwidth-limit <pir>	Disables pir bandwidth limits on the port(s).	13
		bandwidth-limit <egress>	Disables egress bandwidth limits on the port(s).	13
		broadcast-limit	Disables broadcast storm control limit on the port(s).	13
		diffserv	Disables DiffServ on the port(s).	13
		dlf-limit	Disables destination lookup failure (DLF) on the Switch.	13
		egress-set <port-list>	Disables the egress port setting.	13
		flow-control	Disables flow control on the port(s).	13
		ge-spq	Disables strict priority queuing on the Gigabit ports.	13
		gvrp	Disable GVRP on the port(s).	13
		igmp-filtering profile	Disables IGMP filtering.	13
		igmp-group-limit	Disables IGMP group limitation.	13
		igmp-immediate-leave	Disables the IGMP immidiate leave function.	13
		inactive	Enables the port(s) on the Switch.	13
		ingress-check	Disables ingress checking on the port(s).	13
		intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	13
		mirror	Disables port mirroring on the port(s).	13
		multicast-limit	Disables multicast limit on the port(s).	13
		vlan-trunking	Disables VLAN trunking on the port(s).	13
	pvid <vlan-id>		The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.	13
	qos	priority <0 .. 7>	Sets the quality of service priority for an interface.	13

Table 91   interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`speed-duplex`	`<auto|10-half|10-full|100-half|100-full|1000-full>`	Sets the duplex mode (`half` or `full`) and speed (`10`, `100` or `1000` Mbps) of the connection on the interface. Selecting `auto` (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.	13
	`spq`		Sets the port(s) to use Strict Priority Queuing.	13
	`vlan-stacking`	`priority <0-7>`	Sets the priority of the specified port(s) in VLAN stacking.	13
		`role <access | tunnel>`	Sets the VLAN stacking port roles of the specified port(s).	13
		`SPVID <vlan-id>`	Sets the service provider VID of the specified port(s).	13
	`vlan-trunking`		Enables VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.	13
	`weight <wt1> <wt2> ... <wt8>`		A weight value of one to eight is given to each variable from wt 1 to wt 8.	13
	`wrr`		Sets the port(s) to use Weighted Round Robin queuing.	13

38.11.5 interface route-domain Commands

The following table lists the `interface route-domain` commands in configuration mode.

Use these commands to configure the IP routing domains.

Table 92   interface route-domain Commands

COMMAND			DESCRIPTION	PRIVILEGE
`interface route-domain <ip-address>/ <mask-bits>`			Enables a routing domain for configuration.	13
	`exit`		Exits from the interface routing-domain command mode.	13
	`ip`	`igmp <v1|v2>`	Enables IGMP in this routing domain.	13
		`igmp robustness-variable <2-255>`	Sets the igmp robustness variable on the Switch. This variable specifies how susceptible the subnet is to lost packets.	13

Table 92 interface route-domain Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`igmp query-interval`	Sets the igmp query interval on the Switch. This variable specifies the amount of time in seconds between general query messages sent by the router.	13
		`igmp query-max-response-time <1-25>`	Sets the maximum time that the router waits for a response to an general query message.	13
		`igmp last-member-query-interval <1-25>`	Sets the amount of time in seconds that the router waits for a response to a group specific query message.	13
		`rip direction <Outgoing|Incoming|Both|None> version <v1|v2b|v2m>`	Sets the RIP direction in this routing domain as well as the version number.	13
	`no`	`ip igmp`	Disables IP IGMP in this routing domain.	13

38.11.6 config-vlan Commands

The following table lists the `vlan` commands in configuration mode.

Table 93 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION	PRIVILEGE
`vlan <vlan-id>`			Creates a new VLAN group.	13
	`exit`		Leaves the VLAN configuration mode.	13
	`fixed <port-list>`		Specifies the port(s) to be a permanent member of this VLAN group.	13
	`forbidden <port-list>`		Specifies the port(s) you want to prohibit from joining this VLAN group.	13
	`help`		Displays a list of available VLAN commands.	13
	`inactive`		Disables the specified VLAN.	13
	`ip address`	`<ip-address> <mask>`	Sets the IP address of the Switch in the VLAN.	13
		`<ip-address> <mask> manageable`	Sets the IP address of the Switch in the VLAN and allow remote management to this IP address.	13
		`default-gateway <ip-address>`	Sets the default gateway IP address in this VLAN.	13
	`name <name-str>`		Specifies a name for identification purposes.	13

259

Table 93 Command Summary: config-vlan Commands (continued)

COMMAND			DESCRIPTION	PRIVILEG E
	`no`	`fixed <port-list>`	Sets fixed port(s) to normal port(s).	13
		`forbidden <port-list>`	Sets forbidden port(s) to normal port(s).	13
		`inactive`	Enables the specified VLAN.	13
		`ip address <ip-address> <mask>`	Deletes the IP address and subnet mask from this VLAN.	13
		`ip address default-gateway`	Deletes the default gateway from this VLAN.	13
		`untagged <port-list>`	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.	13
	`normal <port-list>`		Specifies the port(s) to dynamically join this VLAN group using GVRP	13
	`untagged <port-list>`		Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.	13

38.12 mvr Commands

The following table lists the `mvr` commands in configuration mode.

Table 94 Command Summary: mvr Commands

COMMAND			DESCRIPTION	PRIVILEG E
`mvr <vlan-id>`			Enters the MVR (Multicast VLAN Registration) configuration mode.	13
	`exit`		Exist from the MVR configuration mode.	13
	`group <name-str> start-address <ip> end-address <ip>`		Sets the multicast group range for the MVR.	13
	`inactive`		Disables MVR settings.	13
	`mode <dynamic| compatible>`		Sets the MVR mode (dynamic or compatible).	13
	`name <name-str>`		Sets the MVR name for identification purposes.	13
	`no`	`group`	Disables all MVR group settings.	13
		`group <name-str>`	Disables the specified MVR group setting.	13
		`inactive`	Enables MVR.	13

Table 94 Command Summary: mvr Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`receiver-port <port-list>`	Disables the receiver port(s).An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
		`source-port <port-list>`	Disables the source port(s).An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
		`tagged <port-list>`	Sets the port(s) to untag VLAN tags.	13
	`receiver-port <port-list>`		Sets the receiver port(s).An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
	`source-port <port-list>`		Sets the source port(s).An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
	`tagged <port-list>`		Sets the port(s) to tag VLAN tags.	13
	`8021p-priority`		Sets the 802.1p priority for the packets belonging to this VLAN group.	13

User and Enable Mode Commands

This chapter describes some commands which you can perform in the User and Enable modes.

39.1 Overview

The following command examples show how you can use User and Enable modes to diagnose and manage your Switch.

39.2 show Commands

These are the commonly used `show` commands.

39.2.1 show system-information

Syntax:

`show system-information`

This command shows the general system information (such as the firmware version and system up time).

An example is shown next.

```
sysname# show system-info

System Name           : GS-2724
System Contact        :
System Location       :
Ethernet Address      : 00:19:cb:00:11:fa
ZyNOS F/W Version     : V3.70(AYC.0)b0 | 03/08/2007
RomRasSize            : 2721784
System up Time        :    94:49:25 (208e20f ticks)
Bootbase Version      : V3.1 | 03/08/2007
ZyNOS CODE            : RAS Mar  8 2007 11:23:31
Product Model         : GS-2724
```

39.2.2 show ip

Syntax:

```
show ip
```

This command displays the IP related information (such as IP address and subnet mask) on all Switch interfaces.

The following figure shows the default interface settings.

```
sysname> show  ip
Out-of-band Management IP Address = 192.168.0.1
Management IP Address
     IP[192.168.0.1], Netmask[255.255.255.0], VID[0]
IP Interface
     IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
sysname>
```

39.2.3 show logging

Syntax:

```
show logging
```

This command displays the system logs. The following figure shows an example.

```
sysname# show logging
   1 Thu Jan  1 00:02:08 1970 PP05 -WARN  SNMP TRAP 3: link up
   2 Thu Jan  1 00:03:14 1970        INFO  adjtime task pause 1 day
   3 Thu Jan  1 00:03:16 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
   4 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 1: warm start
   5 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 3: link up
   6 Thu Jan  1 00:03:16 1970 PINI  INFO  main: init completed
   7 Thu Jan  1 00:00:13 1970 PP26  INFO  adjtime task pause 1 day
   8 Thu Jan  1 00:00:14 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
   9 Thu Jan  1 00:00:14 1970 PINI -WARN  SNMP TRAP 0: cold start
  10 Thu Jan  1 00:00:14 1970 PINI  INFO  main: init completed
  11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
  11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
Clear Error Log (y/n):
```

> ✎ If you clear a log (by entering `y` at the `Clear Error Log (y/n):`prompt), you cannot view it again.

39.2.4 show interface

Syntax:

```
show interface [port-number]
```

This command displays statistics of a port. The following example shows that port 2 is up and the related information.

```
sysname# show interface 2
  Port Info     Port NO.                :2
                Link                    :100M/F
                Status                  :FORWARDING
                LACP                    :Disabled
                TxPkts                  :0
                RxPkts                  :63
                Errors                  :0
                Tx KBs/s                :0.0
                Rx KBs/s                :0.0
                Up Time                 :0:02:33
  TX Packet     Tx Packets              :0
                Multicast               :0
                Broadcast               :0
                Pause                   :0
                Tagged                  :0
  RX Packet     Rx Packets              :63
                Multicast               :0
                Broadcast               :63
                Pause                   :0
                Control                 :0
  TX Collison   Single                  :0
                Multiple                :0
                Excessive               :0
                Late                    :0
  Error Packet  RX CRC                  :0
                Length                  :0
                Runt                    :0
  Distribution  64                      :3
                65 to 127               :44
                128 to 255              :14
                256 to 511              :2
                512 to 1023             :0
                1024 to 1518            :0
                Giant                   :0
sysname#
```

39.2.5 show mac address-table

Syntax:

```
show mac address-table <all <sort>|static>
```

Where

<sort> = Specifies the sorting criteria (MAC, VID or port).

This command displays the MAC address(es) stored in the Switch. The following example shows the static MAC address table.

```
sysname# show mac address-table static
Port      VLAN ID        MAC Address        Type
CPU       1              00:a0:c5:01:23:46  Static
sysname#
```

39.3 ping

Syntax:

```
ping <ip|host-name> < [in-band|out-of-band|vlan <vlan-id> ] [size
-> <0-1472>] [-t]>
```

where

`<ip|host-name>`	=	The IP address or host name of an Ethernet device.
`[in-band|out-of-band|vlan <vlan-id>]`	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs. `out-of-band` refers to the management port while `in-band` means the other ports on the Switch.
`[size <0-1472>]`	=	Specifies the packet size to send.
`[-t]`	=	Sends Ping packets to the Ethernet device indefinitely. Press `[CTRL]+ C` to terminate the Ping process.

This command sends Ping packets to an Ethernet device. The following example sends Ping requests to and displays the replies from an Ethernet device with an IP address of `192.168.1.100`.

```
sysname# ping 192.168.1.100
 sent  rcvd  rate   rtt    avg   mdev    max    min  reply from
    1     1  100      0      0      0      0      0  192.168.1.100
    2     2  100      0      0      0      0      0  192.168.1.100
    3     3  100      0      0      0      0      0  192.168.1.100
sysname#
```

39.4 traceroute

Syntax:

```
traceroute <ip|host-name> [in-band|out-of-band|vlan <vlan-id>][ttl
-> <1-255>] [wait <1-60>] [queries <1-10>]
```

where

`<ip|host-name>`	=	The IP address or host name of an Ethernet device.
`[in-band|out-of-band|vlan <vlan-id>]`	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs.
`[ttl <1-255>]`	=	Specifies the Time To Live (TTL) period.
`[wait <1-60>]`	=	Specifies the time period to wait.
`[queries <1-10>]`	=	Specifies how many tries the Switch performs the traceroute function.

This command displays information about the route to an Ethernet device. The following example displays route information to an Ethernet device with an IP address of `192.168.1.100`.

```
sysname> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
  1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
sysname>
```

39.5 Copy Port Attributes

Use the `copy running-config` command to copy attributes of one port to another port or ports.

Syntax:

```
copy running-config interface port-channel <port> <port-list>
copy running-config interface port-channel <port> <port-list>
-> [active] [name] [speed-duplex] [bpdu-control] [flow-control]
-> [intrusion-lock] [vlan1q] [vlan1q-member] [bandwidth-limit]
-> [vlan-stacking] [port-security] [broadcast-storm-control] [mirroring]
-> [port-access-authenticator] [queuing-method] [igmp-filtering]
-> [spanning-tree] [mrstp] [port-based-vlan]
```

where

`copy running-config interface port-channel <port> <port-list>`	=	Copies all of the possible attributes from one port to another port or ports.
`copy running-config interface port-channel <port> <port-list> [active... ]`	=	Copies only the specified port attributes from one port to another port or ports.

An example is shown next.

- Copy all attributes of port 1 to port 2
- Copy selected attributes (active, bandwidth limit and STP settings) to ports 5-8

```
sysname# copy running-config interface port-channel 1 2
sysname# copy running-config interface port-channel 1 5-8 active
bandwidth-limit spanning-tree
```

39.6 Configuration File Maintenance

The following sections show how to manage the configuration files.

267

39.6.1 Using a Different Configuration File

You can store up to two configuration files on the Switch. Only one configuration file is used at a time. By default the Switch uses the first configuration file (with an index number of 1). You can set the Switch to use a different configuration file. There are two ways in which you can set the Switch to use a different configuration file: restart the Switch (cold reboot) and restart the system (warm reboot).

Use the `boot config` command to restart the Switch and use a different configuration file (if specified). The following example restarts the Switch to use the second configuration file.

```
sysname# boot config 2
```

Use the `reload config` command to restart the system and use a different configuration file (if specified). The following example restarts the system to use the second configuration file.

```
sysname# reload config 2
```

✎   When you use the `write memory` command without specifying a configuration file index number, the Switch saves the changes to the configuration file the Switch is currently using.

39.6.2 Resetting to the Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1 Enter `erase running config` to reset the current running configuration.
2 Enter `write memory` to save the changes to the current configuration file. If you want to reset the second configuration file, use the `write memory` command again with the specified index number.

The following example resets both configuration files to the factory default settings.

```
sysname# erase running-config
sysname# write memory
sysname# write memory 2
```

40

Configuration Mode Commands

This chapter describes how to enable and configure your Switch's features using commands. For more background information, see the feature specific chapters which proceed the commands chapters.

40.1 Change the Out of Band Management IP Address

Use the `ip address` command to change the IP address of the out of band management port on the Switch.

Syntax:

```
ip address <IP Address> <Subnet Mask>
```

An example is shown next.

- Change the out of band Management IP address to 192.168.1.10
- View updated settings.

```
sysname(config)# ip address 192.168.1.10 255.255.255.0
sysname(config)# exit
sysname# show ip
Management IP Address
     IP[192.168.0.2], Netmask[255.255.255.0], VID[0]
IP Interface
     IP[192.168.2.1], Netmask[255.255.255.0], VID[2]
```

See example in for information on how to change the in band management IP address for the Switch.

40.2 Enabling IGMP Snooping

To enable IGMP snooping on the Switch. Enter `igmp-snooping` and press [ENTER]. You can also set how to treat traffic from an unknown multicast group by typing the `unknown-multicast-frame` parameter.

Syntax:

```
igmp-snooping
igmp-snooping 8021p-priority <0-7>
igmp-snooping host-timeout <1-16711450>
igmp-snooping leave-timeout <1-16711450>
igmp-snooping unknown-multicast-frame <drop|flooding>
igmp-snooping reserved-multicast-group <drop|flooding>
```

where

`igmp-snooping`	=	Enables IGMP snooping on the Switch.
`8021p-priority`	=	Sets a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets.
`host-timeout <1-16711450>`	=	Specifies the time out period of the Switch with respect to IGMP report queries. If an IGMP report for a multicast group was not received for a host-timeout period, from a specific port, this port is deleted from the member list of that multicast group.
`leave-timeout <1-16711450>`	=	Specifies the time that the Switch will wait for multicast members to respond to a leave report. If no response happens in the timeout period, the Switch deletes the port from the multicast group.
`unknown-multicast-frame <drop|flooding>`	=	Specifies whether you want to discard packets from unknown multicast groups or whether you want to forward them to all ports.
`reserved-multicast-group <drop|flooding>`	=	Specifies whether you want to discard packets in the reserved multicast groups or whether you want to forward them to all ports.

An example is shown next.

- Enable IGMP snooping on the Switch.
- Set the `host-timeout` and `leave-timeout` values to 30 seconds
- Set the Switch to drop packets from unknown multicast groups.

```
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping host-timeout 30
sysname(config)# igmp-snooping leave-timeout 30
sysname(config)# igmp-snooping unknown-multicast-frame drop
```

40.3 Configure IGMP Filter

Use the following commands in the config mode to configure IGMP filtering profiles.

Syntax:

```
igmp-filtering
igmp-filtering profile <name> start-address <ip> end-address <ip>
```

where

`igmp filtering`	=	Enables IGMP filtering on the Switch
`profile <name>`	=	Specifies a name (up to 32 alphanumeric characters) for this IGMP profile. If you want to edit an existing IGMP profile enter the existing profile name followed by `start-address` and `end-address` parameters.
`start-address`	=	Specifies the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile. IP address in the range 224.0.0.0 to 239.255.255.255 are used for IP multicasting.
`end-address`	=	Specifies the ending multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile. IP address in the range 224.0.0.0 to 239.255.255.255 are used for IP multicasting.

An example is shown next.

- Enable IGMP filtering on the Switch.
- Create an IGMP filtering profile **filter1** and specify the multicast IP addresses in the range **224.255.255.0** to **225.255.255.255** to belong to this profile.

```
sysname(config)# igmp-filtering
sysname(config)# igmp-filtering profile filter1 start-address
224.255.255.0 end-address 225.255.255.255
```

40.4 Enabling STP

Use the `spanning-tree` or the `mrstp` commands to enable and configure STP on the Switch. The difference between the commands is that `spanning-tree` only allows you to set up one spanning tree configuration and the `mrstp` command allows you to set up multiple ones.

Syntax:

```
spanning-tree
spanning-tree priority <0-61440>
spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>
spanning-tree <port-list> path-cost <1-65535>
spanning-tree <port-list> priority <0-255>
```

and

```
mrstp <treeIndex> <cr>
mrstp <treeIndex> priority <0-61440>
mrstp <treeIndex> hello-time <1-10> maximum-age <6-40> forward-delay
-> <4-30>
mrstp interface <port-list> <cr>
mrstp interface <port-list> path-cost <1-65535>
mrstp interface <port-list> priority <0-255>
mrstp interface <port-list> treeIndex <1-4>
```

where

`spanning-tree`	=	Enables STP on the Switch.
`mrstp <treeIndex>`		Enables a specific tree configuration.
`priority <0-61440>`	=	Specifies the bridge priority for the Switch. The lower the numeric value you assign, the higher the priority for this bridge.
		Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch.
		Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
`hello-time <1-10>`	=	Specifies the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
`maximum-age <6-40>`	=	Specifies the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network.
`forward-delay <4-30>`	=	Specifies the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
`<port-list> path-cost <1-65535>`	=	Enables STP on the specified ports.
		Specifies the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge.
`<port-list> priority <0-255>`	=	Specifies the priority for each port.
		Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first.
`<port-list> treeIndex <1-4>`	=	Specifies which STP configuration these ports will participate in. (`mrstp` command only).

An example using `spanning-tree` command is shown next.

- Enable STP on the Switch.
- Set the bridge priority of the Switch to 0.
- Set the Hello Time to 4, Maximum Age to 20 and Forward Delay to 15 on the Switch.

272

- Enable STP on port 5 with a path cost of 150.
- Set the priority for port 5 to 20.

```
sysname(config)# spanning-tree priority 0
sysname(config)# spanning-tree hello-time 4 maximum-age 20 forward-delay
15
sysname(config)# spanning-tree 5 path-cost 150
sysname(config)# spanning-tree 5 priority 20
```

40.5 no Command Examples

These are the commonly used command examples that belong to the no group of commands. The no group commands are commands which are preceded by keyword no. This command negates the intended action of the command. In most cases the no command disables, resets or clears settings. There are cases, however, where the no command can activate features. This section shows some uses of these commands.

40.5.1 Disable Commands

Use the no command to disable features on the Switch.

Syntax:

```
no spanning-tree
no mirror-port
```

Disables STP on the Switch.

Disables port mirroring on the Switch.

40.5.2 Resetting Commands

Use the no command to reset settings to their default values.

Syntax:

```
no https timeout
```

Resets the https session timeout to default.

An example is shown next. The session timeout is reset to 300 seconds.

```
sysname(config)# no https timeout
  Cache timeout 300
```

40.5.3 Re-enable commands

The no command can also be used to re-enable features which have been disabled.

Syntax:

```
no ip route <ip> <mask> inactive
```

where

    `<ip> <mask> inactive` = Re-enables an ip route with the specified IP address and subnet mask.

An example is shown next.

- Enable the IP route with the IP address of 192.168.11.1 and subnet mask of 255.255.255.0. This ip route must have already been created and made inactive prior to re-enable command being applied.

```
sysname(config)# no ip route 192.168.11.1 255.255.255.0 inactive
```

40.5.4 Other Examples of no Commands

In some cases the `no` command can disable a feature, disable an option of a feature or disable a feature on a port by port basis.

40.5.4.1 no trunk

Syntax:

```
no trunk <T1|T2|T3|T4|T5|T6>
no trunk <T1|T2|T3|T4|T5|T6> lacp
no trunk <T1|T2|T3|T4|T5|T6> interface <port-list>
```

where

`<T1|T2|T3|T4|T5|T6>`	=	Disables the trunk group.
`<T1|T2|T3|T4|T5|T6> lacp`	=	Disables LACP in the trunk group.
`<T1|T2|T3|T4|T5|T6> interface <port-list>`	=	Removes ports from the trunk group.

An example is shown next.

- Disable trunk one (T1).
- Disable LAPC on trunk three (T3).
- Remove ports one, three, four and five from trunk two (T2).

```
sysname(config)# no trunk T1
sysname(config)# no trunk T3 lacp
sysname(config)# no trunk T2 interface 1,3-5
```

40.5.4.2 no port-access-authenticator

Syntax:

```
no port-access-authenticator
no port-access-authenticator <port-list> reauthenticate
no port-access-authenticator <port-list>
```

where

	=	Disables port authentication on the Switch.
`<port-list> reauthenticate`	=	Disables the re-authentication mechanism on the listed port(s).
`<port-list>`	=	Disables authentication on the listed ports.

An example is shown next.

- Disable authentication on the Switch.
- Disable re-authentication on ports one, three, four and five.
- Disable authentication on ports one, six and seven.

Figure 124   no port-access-authenticator Command Example

```
sysname(config)# no port-access-authenticator
sysname(config)# no port-access-authenticator 1,3-5 reauthenticate
sysname(config)# no port-access-authenticator 1,6-7
```

40.5.4.3 no ssh

Syntax:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <host-ip>
no ssh known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]
```

where

`key <rsa1|rsa|dsa>`	=	Disables the secure shell server encryption key. Your Switch supports SSH versions 1 and 2 using RSA and DSA authentication.
`known-hosts <host-ip>`	=	Removes a specific remote host from the list of all known hosts.
`known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]`	=	Removes remote known hosts with a specified public key type (1024-bit RSA1, RSA or DSA).

An example is shown next.

- Disable the secure shell RSA1 encryption key.
- Remove the remote host with IP address 172.165.1.8 from the list of known hosts.
- Remove the remote host with IP address 172.165.1.9 and with an SSH-RSA encryption key from the list of known hosts.

```
sysname(config)# no ssh key rsa1
sysname(config)# no ssh known-hosts 172.165.1.8
sysname(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

40.6 Static Route Commands

You can create and configure static routes on the Switch by using the `ip route` command.

Syntax:

```
ip route <ip> <mask> <next-hop-ip>
ip route <ip> <mask> <next-hop-ip> [metric <metric>][name <name>]
--> [inactive]
```

where

`<ip>`	=	Specifies the network IP address of the final destination.
`<mask>`	=	Specifies the subnet mask of this destination.
`<next-hop-ip>`	=	Specifies the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
`[metric <metric>]`	=	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
`[name <name>]`	=	Specifies a descriptive name (up to 32 printable ASCII characters) for identification purposes.
`[inactive]`	=	Deactivates a static route

An example is shown next.

- Create a static route with the destination IP address of 172.21.1.104, subnet mask of 255.255.0.0 and the gateway IP address of 192.168.1.2.
- Assigns a metric value of 2 to the static route.
- Assigns the name "route1" to the static route.

```
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 metric 2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 name route1
```

40.7 Enabling MAC Filtering

You can create a filter to drop packets based on the MAC address of the source or the destination.

Syntax:

```
mac-filter name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>
```

where

`name <name>`	=	Names the filtering rule.
`mac <mac-addr>`	=	Specifies the MAC address you want to filter.
`vlan <vlan-id>`	=	Specifies which VLAN this rule applies to.
`drop <src/dst/both>`	=	Selects the behavior of the rule.

- src - drop packets coming from the specified MAC address
- dst- drop packets going to the specified MAC address
- both - drop packets coming from or going to the specified MAC address

An example is shown next.

- Create a filtering rule called "filter1".
- Drop packets coming from and going to MAC address 00:12:00:12:00:12 on VLAN.

```
sysname(config)# mac-filter name filter 1
sysname(config)# mac-filter name filter 1 mac 00:12:00:12:00:12 vlan 1 drop
both
```

40.8 Enabling Trunking

To create and enable a trunk, enter `trunk` followed by the ports which you want to group and press [ENTER].

Syntax:

```
trunk <T1|T2|T3|T4|T5|T6>
trunk <T1|T2|T3|T4|T5|T6> interface <port-list>
trunk <T1|T2|T3|T4|T5|T6> lacp
```

where

`<T1|T2|T3|T4|T5|T6>`	=	Enables the trunk.
`<T1|T2|T3|T4|T5|T6> interface <port-list>`	=	Places ports in the trunk.
`<T1|T2|T3|T4|T5|T6> lacp`	=	Enables LACP in the trunk.

An example is shown next.

- Create trunk 1 on the Switch.
- Place ports 5-8 in trunk 1.

- Enable dynamic link aggregation (LACP) on trunk 1.

```
sysname(config)# trunk t1
sysname(config)# trunk t1 interface 5-8
sysname(config)# trunk t1 lacp
```

40.9 Enabling Port Authentication

To enable a port authentication, you need to specify your RADIUS server details and select the ports which require external authentication. You can set up multiple RADIUS servers and specify how the Switch will process authentication requests.

40.9.1 RADIUS Server Settings

Configuring multiple RADIUS servers is only available via the command interpreter mode. Use the `radius-server` command to set up your RADIUS server settings.

Syntax:

```
radius-server host <index> <ip>
radius-server host <index> <ip> [acct-port <socket-number>] [key
--> <key-string>]
radius-server timeout <1-1000>
radius-server mode <priority|round-robin>
```

where

`radius-server host <index> <ip>`	=	Specifies the IP address of the RADIUS server.
`[acct-port <socket-number>]`	=	Changes the UDP port of the RADIUS server from the default (1812).
`[key <key-string>]`	=	Specifies a password (up to 32 alphanumeric characters) as the key to be shared between the RADIUS server and the Switch.

`radius-server timeout <1-1000>`	=	Specifies the timeout period (in seconds) the Switch will wait for a response from a RADIUS server. If 2 RADIUS servers are configured, this is the total time the Switch will wait for a response from either server.
`mode <priority|round-robin>`	=	Specifies the way the Switch will process requests from the clients to the RADIUS server. (Only applicable with multiple RADIUS servers configured.)
		`priority` - When a client sends an authentication request through the Switch to the RADIUS server. The Switch will forward the request to the RADIUS server. If no response within half the timeout period, it will forward the request to the second RADIUS server.
		`round-robin` - When a client sends an authentication request through the Switch to the RADIUS server. The Switch will forward the request to the first RADIUS server. If there is no response within the timeout period, the request times out. The client sends an authentication request again and the Switch forwards the request to the second RADIUS server.

See for an example.

40.9.2 Port Authentication Settings

Use the `port-access-authenticator` command to configure port security on the Switch.

Syntax:

```
port-access-authenticator
port-access-authenticator <port-list>
port-access-authenticator <port-list> reauthenticate
port-access-authenticator <port-list> reauth-period <reauth-period>
```

where

`port-access-authenticator`	=	Enables port authentication on the Switch.
`port-access-authenticator <port-list>`	=	Specifies which ports require authentication.
`reauthenticate`	=	Enables reauthentication on the port.
`reauth-period <reauth-period>`	=	Specifies how often a client has to re-enter his or her username and password to stay connected to the port.

An example is shown next.

- Specify RADIUS server 1 with IP address 10.10.10.1, port 1890 and the string `secretKey` as the password. See for more information on RADIUS server commands.

- Specify the timeout period of 30 seconds that the Switch will wait for a response from the RADIUS server.
- Enable port authentication on ports 4 to 8.
- Activate reauthentication on the ports.
- Specify 1800 seconds as the interval for client reauthentication.

```
sysname(config)# radius-server host 1 10.10.10.1 acct-port 1890 key
--> secretKey
sysname(config)# radius-server timeout 30
sysname(config)# port-access-authenticator
sysname(config)# port-access-authenticator 4-8
sysname(config)# port-access-authenticator 4-8 reauthenticate
sysname(config)# port-access-authenticator 4-8 reauth-period 1800
```

41

Interface Commands

These are some commonly used configuration commands that belong to the `interface` group of commands.

41.1 Overview

The interface commands allow you to configure the Switch on a port by port basis.

41.2 Interface Command Examples

This section provides examples of some frequently used interface commands.

41.2.1 interface port-channel

Use this command to enable the specified ports for configuration. Indicate multiple, non-sequential ports separated by a comma. Use a dash to specify a port range.

Syntax:

```
interface port-channel <port-list>
```

An example is shown next.

- Enter the configuration mode.
- Enable ports 1, 3, 4 and 5 for configuration.
- Begin configuring for those ports.

```
sysname# config
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)#
```

41.2.2 bpdu-control

Syntax:

```
bpdu-control <peer|tunnel|discard|network>
```

where

`<peer|tunnel|discard|` `network>`	=	Type `peer` to process any BPDUs received on these ports.
		Type `tunnel` to forward BPDUs received on these ports.
		Type `discard` to drop any BPDUs received on these ports.
		Type `network` to process a BPDU with no VLAN tag and forward a tagged BPDU.

An example is shown next.

- Enable ports 1, 3, 4 and 5 for configuration.
- Set the BPDU control to `tunnel`, to forward BPDUs received on ports one, three, four and five.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# bpdu-control tunnel
sysname(config-interface)#
```

41.2.3 broadcast-limit

Syntax:

```
broadcast-limit
broadcast-limit <pkt/s>
```

where

	=	Enables broadcast storm control limit on the Switch.
`<pkt/s>`	=	Limits how many broadcast packet the interface receives per second.

An example is shown next.

- Enable port one for configuration.
- Enable broadcast control.
- Set how many broadband packets the interface receives per second.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 21
```

41.2.4 bandwidth-limit

The `bandwidth-limit` command enables bandwidth control on the Switch.

Syntax:

```
bandwidth-limit
bandwidth-limit pir <Kbps>
bandwidth-limit cir <Kbps>
bandwidth-limit egress <Kbps>
```

where

`pir <Kbps>`	=	Sets the maximum bandwidth allowed for incoming traffic.
`cir <Kbps>`	=	Sets the guaranteed bandwidth allowed for incoming traffic.
`egress <Kbps>`	=	Sets the maximum bandwidth allowed for outgoing traffic (`egress`) on the Switch.

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control.
- Set the outgoing traffic bandwidth limit to 5000Kbps.
- Set the guaranteed bandwidth allowed for incoming traffic to 4000Kbps.
- Set the maximum bandwidth allowed for incoming traffic to 8000Kbps.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit
sysname(config-interface)# bandwidth-limit egress 5000
sysname(config-interface)# bandwidth-limit cir 4000
sysname(config-interface)# bandwidth-limit pir 8000
```

41.2.5 mirror

The `mirror` command enables port mirroring on the interface.

Syntax:

```
mirror
mirror dir <ingress|egress|both>
```

where

`dir <ingress|egress|both>`	=	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic.
		Port mirroring copies traffic from one or all ports to another or all ports for external analysis.

An example is shown next.

- Enable port mirroring.
- Enable the monitor port 3.
- Enable ports 1, 4, 5 and 6 for configuration.
- Enable port mirroring on the ports.

- Enable port mirroring for outgoing traffic. Traffic is copied from ports 1, 4, 5 and 6 to port three in order to examine it in more detail without interfering with the traffic flow on the original ports.

```
sysname(config)# mirror-port
sysname(config)# mirror-port 3
sysname(config)# interface port-channel 1,4-6
sysname(config-interface)# mirror
sysname(config-interface)# mirror dir egress
```

41.2.6 gvrp

Syntax:

```
gvrp
```

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local switch.

An example is shown next.

- Enable the IEEE 802.1Q tagged VLAN command to configure tagged VLAN for the Switch.
- Enable ports one, three, four and five for configuration.
- Enable GVRP on the interface.

```
sysname(config)# vlan1q gvrp
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# gvrp
```

41.2.7 ingress-check

The `ingress-check` command enables the device to discard incoming frames for VLANs that do not have this port as a member.

Syntax:

```
ingress-check
```

An example is shown next.

- Enable ports 1, 3, 4 and 5 for configuration.
- Enable ingress checking on the interface.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
```

41.2.8 frame-type

Syntax:

```
frame-type <all|tagged|untagged>
```

where

`<all|tagged|untagged>`	=	Choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Enable ingress checking on the ports.
- Enable tagged frame-types on the interface.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
sysname(config-interface)# frame-type tagged
```

41.2.9 weight

Syntax:

```
weight <wt1> <wt2> ... <wt8>
```

where

`<wt1> <wt2> ... <wt8>`	=	Sets the interface WFQ weighting. A weight value of one to eight is given to each variable from `wt 1` to `wt 8`.

An example is shown next.

- Enable WRR queuing on ports 2 and 6 to 8.
- Enable port 2 and ports 6 to 8 for configuration.
- Set the queue weights from Q0 to Q7.

```
sysname# configure
sysname(config)# interface port-channel 2,6-8
sysname(config-interface)# wrr
sysname(config-interface)# weight 8 7 6 5 4 3 2 1
```

41.2.10 egress set

Syntax:

```
egress set <port-list>
```

where

`<port-list>`	=	Sets the outgoing traffic port list for a port-based VLAN.

An example is shown next.

- Enable port-based VLAN tagging on the Switch.
- Enable ports one, three, four and five for configuration.

- Set the outgoing traffic ports as the CPU (0), seven (7) and eight (8).

```
sysname(config)# vlan-type port-based
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# egress set 0,7,8
```

41.2.11 qos priority

Syntax:

```
qos priority <0 .. 7>
```

where

    <0 .. 7>   =   Sets the quality of service priority for a port.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the IEEE 802.1p quality of service priority as four (4).

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# qos priority 4
```

41.2.12 name

Syntax:

```
name <port-name-string>
```

where

    <port-name-string>   =   Sets a name for your port interface.

An example is shown next.

- Enable port one for configuration.
- Set a name for the port.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# name Test
```

41.2.13 speed-duplex

Syntax:

```
speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>
```

where

<auto|10-half|10-full|100-half|100-full|1000-full>	=	Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the port. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.

An example is shown next.

- Enable ports one, three, four and five for configuration.
- Set the speed to 100 Mbps in half duplex mode.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# speed-duplex 100-half
```

41.2.14 test

You can perform an interface loopback test on specified ports. The test returns `Passed!` or `Failed!`

An example is shown next.

- Select ports 3-6 for internal loopback test.
- Execute the test command.
- View the results.

```
sysname(config)# interface port-channel 3-6
sysname(config-interface)# test 3-6
Testing internal loopback on port 3 :Passed!
  Ethernet Port 3 Test ok.
Testing internal loopback on port 4 :Passed!
  Ethernet Port 4 Test ok.
Testing internal loopback on port 5 :Passed!
  Ethernet Port 5 Test ok.
Testing internal loopback on port 6 :Passed!
  Ethernet Port 6 Test ok.
```

41.3 Interface no Command Examples

Similar to the no commands in the Enable and Config modes, the no commands for the Interface sub mode also disable certain features. In this mode, however, this takes place on a port by port basis.

41.3.1 no bandwidth-limit

You can disable bandwidth limit on port 1 simply by placing the `no` command in front of the `bandwidth-limit` command.

Syntax:

```
no bandwidth-limit
```

An example is shown next:

- Disable bandwidth limit on port1

```
sysname(config)# interface port-channel 1
sysname(config-interface)# no bandwidth-limit
```

IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands.

42.1 Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

1 Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the Switch.

- Use the `vlan <vlan-id>` command to configure or create a VLAN on the Switch. The Switch automatically enters the `config-vlan` mode.Use the `inactive` command to deactivate the VLAN(s).

- Use the `interface port-channel <port-list> command` to enter the config-interface mode to set the VLAN settings on a port, then use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list to that specific port in the PVID table.

- Use the `exit` command when you are finished configuring the VLAN.

```
sysname (config)# vlan 2000
sysname (config-vlan)# name up1
sysname (config-vlan)# fixed 5-8
sysname (config-vlan)# no untagged 5-8
sysname (config-vlan)# exit
sysname (config)# interface port-channel 5-8
sysname (config-interface)# pvid 2000
sysname (config-interface)# exit
```

2 Configure your management VLAN.

- Use the `vlan <vlan-id>` command to create a VLAN (VID 3 in this example) for managing the Switch, and the Switch will activate the new management VLAN.

- Use the `inactive` command to disable the new management VLAN.

```
sysname (config)# vlan 3
sysname (config-vlan)# inactive
```

42.2 Global VLAN1Q Tagged VLAN Configuration Commands

This section shows you how to configure and monitor the IEEE 802.1Q Tagged VLAN.

42.2.1 GARP Status

Syntax:

```
show garp
```

This command shows the Switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
sysname# show garp
GARP Timer
-----------------------
Join Timer = 200
Leave Timer = 600
Leave All Timer = 10000
sysname#
```

42.2.2 GARP Timer

Syntax:

```
garp join <msec> leave <msec> leaveall <msec>
```

where

join <msec>	=	This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds.
leave <msec>	=	This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.
leaveall <msec>	=	This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.

This command sets the Switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
sysname (config)# garp join 300 leave 800 leaveall 11000
```

42.2.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the Switch's GVRP settings.

An example is shown next.

```
sysname# show vlan1q gvrp
GVRP Support
---------------------
gvrpEnable = YES
sysname #
```

42.2.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

This command turns on GVRP in order to propagate VLAN information beyond the Switch.

42.2.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

This command turns off GVRP so that the Switch does not propagate VLAN information to other switches.

42.3 Port VLAN Commands

You must configure the Switch's port VLAN settings in config-interface mode.

42.3.1 Set Port VID

Syntax:

```
pvid <VID>
```

where

`<VID>`	=	Specifies the VLAN number between 1 and 4094.

This command sets the default VLAN ID on the port(s).

The following example sets the default VID to 200 on ports 1 to 5.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# pvid 200
```

42.3.2 Set Acceptable Frame Type

Syntax:

```
frame-type <all|tagged|untagged>
```

where

`<all|tagged| untagged>`	=	Specifies all Ethernet frames (tagged and untagged), only tagged Ethernet frames or only untagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets ports 1 to 5 to accept only tagged frames.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# frame-type tagged
```

42.3.3 Enable or Disable Port GVRP

Use the gvrp command to enable GVRP on the port(s). Use the no gvrp command to disable GVRP.

The following example turns off GVRP for ports 1 to 5.

```
sysname (config)# interface port-channel 1-5
sysname (config-interface)# no gvrp
```

42.3.4 Modify Static VLAN

Use the following commands in the config-vlan mode to configure the static VLAN table.

Syntax:

```
vlan <vlan-id>
fixed <port-list>
forbidden <port-list>
name <name-str>
normal <port-list>
untagged <port-list>
no fixed <port-list>
no forbidden <port-list>
no untagged <port-list>
```

where

`<vlan-id>`	=	The VLAN ID [1 – 4094].
`<name-str>`	=	A name to identify the SVLAN entry.
`<port-list>`	=	This is the Switch port list.

- Enter `fixed` to register the `<port-list>` to the static VLAN table with `<vlan-id>`.
- Enter `normal` to confirm registration of the `<port-list>` to the static VLAN table with `<vlan-id>`.
- Enter `forbidden` to block a `<port-list>` from joining the static VLAN table with `<vlan-id>`.
- Enter `no fixed` or `no forbidden` to change `<port-list>` to normal status.
- Enter `untagged` to send outgoing frames without a tag.
- Enter `no untagged` to tag outgoing frames.

42.3.4.1 Modify a Static VLAN Table Example

The following example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

```
sysname (config)# vlan 2000
sysname (config-vlan)# fixed 1-5
sysname (config-vlan)# untagged 1-5
```

42.3.4.2 Forwarding Process Example

42.3.4.2.1 Tagged Frames

1 First the Switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames.
2 The Switch then checks the VID in a frame's tag against the SVLAN table.
3 The Switch notes what the SVLAN table says (that is, the SVLAN tells the Switch whether or not to forward a frame and if the forwarded frames should have tags).
4 Then the Switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

42.3.4.2.2 Untagged Frames

1 An untagged frame comes in from the LAN.
2 The Switch checks the PVID table and assigns a temporary VID of 1.
3 The Switch ignores the port from which the frame came, because the Switch does not send a frame to the port from which it came. The Switch also does not forward frames to "forbidden" ports.
4 If after looking at the SVLAN, the Switch does not have any ports to which it will send the frame, it won't check the port filter.

42.3.5 Delete VLAN ID

Syntax:

```
no vlan <vlan-id>
```

where

    `<vlan-id>`   =   The VLAN ID [1 – 4094].

This command deletes the specified VLAN ID entry from the static VLAN table. The following example deletes entry 2 in the static VLAN table.

```
sysname (config)# no vlan 2
```

42.4 Enable VLAN

Syntax:

```
vlan <vlan-id>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

42.5 Disable VLAN

Syntax:

```
vlan <vlan-id> inactive
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

42.6 Show VLAN Setting

Syntax:

```
show vlan
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

- VID is the VLAN identification number.
- Status shows whether the VLAN is static or active.
- Elap-Time is the time since the VLAN was created on the Switch.

- The TagCtl section of the last column shows which ports are tagged and which are untagged.

```
sysname# show vlan
  The Number of VLAN:    3
  Idx. VID   Status    Elap-Time    TagCtl
  ---- ----  --------  ------------ ------------------------
  1   1     Static    0:12:13     Untagged :1-2
                                   Tagged   :

  1  100    Static    0:00:17     Untagged :
                                   Tagged   :1-4

  1  200    Static    0:00:07     Untagged :1-2
                                   Tagged   :3-8
```

Multicast VLAN Registration Commands

This chapter shows you how to use Multicast VLAN Registration (mvr) commands.

43.1 Overview

Use the mvr commands in the configuration mode to create and configure multicast VLANs.

✎ If you want to enable IGMP snooping see Section 40.2 on page 269.

43.2 Create Multicast VLAN

Use the following commands in the config-mvr mode to configure a multicast VLAN group.

Syntax:

```
mvr <vlan-id>
mvr <vlan-id> source-port <port-list>
mvr <vlan-id> receiver-port <port-list>
mvr <vlan-id> inactive
mvr <vlan-id> mode <dynamic|compatible>
mvr <vlan-id> name <name-str>
mvr <vlan-id> tagged <port-list>
mvr <vlan-id> group <name-str> start-address <ip> end-address <ip>
mvr <vlan-id> exit
```

where

`<vlan-id>`	=	The VLAN ID [1 – 4094].
`source-port <port-list>`	=	Specifies the MVR source ports which send and receive multicast traffic.
`receiver-port <port-list>`	=	Specifies the MVR receiving ports which only receive multicast traffic.
`name <name-str>`	=	A name to identify the multicast VLAN group.

`mode`
`<dynamic|compati`
`ble>`
	=	Specifies dynamic (sends IGMP reports to all source ports in the multicast VLAN) or compatible (does not send IGMP reports).

`group name` `<name-str>`	=	A name to identify the MVR IP multicast group.
`start-address` `<ip>`	=	Specifies the starting IP multicast address of the multicast group in dotted decimal notation.
`end-address <ip>`	=	Specifies the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the start-address if you want to configure only one IP address for the multicast group.

- Enter MVR mode. Create a multicast VLAN with the name `multiVlan` and the VLAN ID of 3.
- Specify source ports 2, 3, 5 and receiver ports 6-8.
- Specify dynamic mode for the multicast group.
- Configure MVR multicast group addresses by the name of `ipgroup`.
- Exit MVR mode.

See the following example.

```
sysname(config)# mvr 3 name multivlan
sysname(config-mvr)# source-port 2,3,5 receiver-port 6-8
sysname(config-mvr)# mode dynamic
sysname(config-mvr)# group ipgroup start-address 224.0.0.1 end-address
--> 224.0.0.255
sysname(config-mvr)# exit
```

44

Routing Domain Command Examples

44.1 interface route-domain

Syntax:

```
interface route-domain <ip-address>/<mask-bits>
```

where

`<ip-address>`	=	This is the IP address of the Switch in the routing domain. Specify the IP address is dotted decimal notation. For example, 192.168.1.1.
`<mask-bits>`	=	The number of bits in the subnet mask. Enter the subnet mask number preceded with a "/". To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).

Use this command to enable/create the specified routing domain for configuration.

An example is shown next.

- Enter the configuration mode.
- Enable default routing domain (the 192.168.1.1 subnet) for configuration.
- Begin configuring for this domain.

```
sysname# config
sysname(config)# interface route-domain 192.168.1.1/24
cmd interface route domain
 192.168.1.1 255.255.255.0
sysname(config-if)#
```

45

Troubleshooting

This chapter covers potential problems and possible remedies.

45.1 Problems Starting up the Switch

Table 95   Troubleshooting the Start-Up of Your Switch

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the Switch.	Check the power connection and make sure the power source is turned on.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

45.2 Problems Accessing the Switch

Table 96   Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the Switch using Telnet.	Make sure the ports are properly connected.
	You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.
	Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to Chapter 29 on page 193 for details.
I cannot access the web configurator.	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
	If you have configured more than one IP interface, make sure another administrator is NOT logged into the web configurator on a different IP interface using the same account.
	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to Chapter 29 on page 193 for details.
	Your computer's and the Switch's IP addresses must be on the same subnet.
	See Appendix C on page 313 to check that pop-up windows, JavaScripts and Java permissions are allowed.

45.3 Problems with the Password

Table 97   Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the Switch.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password. See Section 4.6.1 on page 55.

PART VII
Appendices and Index

303

Product Specifications

This section describes the general software features of the Switch.

Table 98   Firmware Features

FEATURE	DESCRIPTION
IP Routing Domain	An IP interface (also known as an IP routing domain) is not bound to a physical port. Configure an IP routing domain to allow the Switch to route traffic between different networks.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
VLAN Stacking	Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the Switch assign IP addresses, an IP default gateway and DNS servers to computers on your network.
IGMP Snooping	The Switch supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your Switch.
Differentiated Services (DiffServ)	With DiffServ, the Switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Classifier and Policy	You can create a policy to define actions to be performed on a traffic flow grouped by a classifier according to specific criteria such as the IP address, port number or protocol type, etc.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. Two scheduling services are supported: Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR). This allows the Switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.
Port Cloning	Port cloning allows you to copy attributes from one port to another port or ports.

Table 98 Firmware Features (continued)

FEATURE	DESCRIPTION
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
RIP	RIP (Routing Information Protocol) allows a routing device to exchange routing information with other routers.
RSTP (Rapid Spanning Tree Protocol) / MRSTP (Multiple RSTP)	RSTP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other RSTP-compliant switches in your network to ensure that only one path exists between any two stations on the network. MRSTP allows you to configure multiple RSTP configurations and assign ports to each tree.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. For redundancy, multiple RADIUS servers can be configured.
Device Management	Use the web configurator to easily configure the rich range of features on the Switch.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
Cluster Management	Cluster management (also known as iStacking) allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

The following table lists the product specifications.

Table 99 General Product Specifications

Interface		20 1000Base-Tx ports
		4 GbE Dual Personality interfaces (Each interface has one 1000Base-T copper port and one Small Form-Factor Pluggable (SFP) fiber port, with one port active at a time.)
		One local console, RS-232
		One 100Base-Tx port, RJ-45, for out-of-band management
		Auto-negotiation
		Auto-MDIX
		Compliant with IEEE 802.3ad/u/x
		Back pressure flow control for half duplex
		Flow control for full duplex (IEEE 802.3x)
		Rate limiting at 64-Kbps steps
Layer 2 Features	Bridging	8K MAC addresses
		Static MAC address filtering by source/destination
		Broadcast storm control
		Static MAC address forwarding
	Switching	Switching fabric: 48 Gbps, non-blocking
		Max. Frame size: 1522 bytes
		Forwarding frame: IEEE 802.3, IEEE 802.1Q, Ethernet II, PPPoE
		Prevent the forwarding of corrupted packets
	STP	IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
		Multiple Rapid Spanning Tree capability (4 configurable trees)
	QoS	IEEE 802.1p with 8 priority queues per port
		Rule-based classification
		Rule-based shaping
		DSCP
		Bandwidth control
		Rate limiting in 64-kbps increments
		IGMP Snooping
	VLAN	Port-based VLAN setting
		Tag-based (IEEE 802.1Q) VLAN
		Number of VLAN: 4K, 256 static maximum
		Supports GVRP
		Double tagging for VLAN stacking
	Port Aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking
		Six groups (up to 8 ports each)
	Port mirroring	All ports support port mirroring
		Support port mirroring per IP/TCP/UDP
	Bandwidth control	Supports rate limiting at 64K increment

Table 99   General Product Specifications (continued)

Layer 3 Features	IP Capability	IPV4 support 8 IP routing domains 1K IP address table 1K routing entries Wire speed IP forwarding
	Routing protocols	Unicast: RIP-V1/V2 Multicast: IGMP V1/V2 8 Static Routes
	IP services	DHCP server/relay
Performance		Wire-speed throughput 1488000 pps for 1000Base-T, 64-byte packet 148800 pps for 100Base-TX, 64-byte packet Non-blocking 48-Gbps switching fabric
Availability		IEEE 802.3ad (LACP): 6 groups, 8 ports/groups randomly selected IEEE 802.1D (STP) IEEE 802.1w (RSTP) Supports ZyXEL BPS backup power system
Security		Static MAC address filtering Limiting number of dynamic addresses per port IEEE 802.1x port-based authentication Port based VLAN 802.1Q VLAN 256 static VLAN GVRP, automatic member registration SSH SSL Wire speed filtering per MAC/IP/TCP/UDP Wire speed rate limiting per MAC/IP/TCP/UDP Wire speed mirroring per MAC/IP/TCP/UDP
Access Control List (ACL)		Based on Port Based on MAC+VLAN ID Based on IP Address (Source/Destination) Based on L3 Protocol category Based on TCP/UDP port number

Table 100 Management Specifications

System Control	Alarm/Status surveillance
	Automatic alarm and status report
	Alarm/event history
	LED indication for alarm and system status
	Performance monitoring
	Line speed
	Four RMON groups 1, 2, 3, 9 (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis
	Throughput monitoring
	Transmit and receive of ICMP packets
	Port mirroring and aggregation
	Spanning Tree Protocol
	IGMP snooping
	Firmware upgrade and download through FTP/TFTP
	DHCP server/relay
	Security and Memory Backup
	Login authorization and security levels (Privileges assigned via CLI or via RADIUS server)
	Self diagnostics
	Non-volatile memory for system database storage
	FLASH memory
	Support MIB community string, community access privilege, Trap IP setting
Network Management	CLI through console port and Telnet
	RS-232C (DB-9) port for local management
	Firmware upgrade, configuration backup/restore via FTP
	Text-based configuration profile for massive deployment
	Web-based management
	iStacking^{TM}/Clustering: up to 24 switches can be managed by one IP address
	SNMP v1/v2c/v3
	Trap transmission: up to 4 destinations
	RMON groups (history, statistics, alarms and events)
MIB	RFC1155 SMI
	RFC1157 SNMP v1
	RFC1213 MIB II
	RFC2011 IP MIP
	RFC2012 TCP MIB
	RFC2013 UDP MIB
	RFC1493 Bridge MIB
	RFC1643 Ethernet MIB
	RFC1757 Four groups of RMON
	RFC2674 Bridge MIB extension, SNMP v2, SNMP v2c

Table 101 Physical and Environmental Specifications

LEDs	Per Switch: BPS, PWR, SYS, ALM Per Gigabit Ethernet/mini-GBIC port: 100, 1000/LNK, ACT Per mini-GBIC port: LNK, ACT Per Management port: 10, 100
Dimension	Standard 19" rack mountable 438 mm (W) x 300 mm (D) x 44.45 mm (H)
Weight	4.2 kg
Temperature	Operating: 0º C ~ 45º C (32º F ~ 113º F) Storage: -25º C ~ 70º C (14º F ~ 158º F)
Humidity	10 ~ 90% (non-condensing)
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

Table 102 Power Specifications

MODEL	SPECIFICATIONS
AC	100-240 VAC 50/60 Hz, 1.5 A max.
DC	-48 VDC ~ -60 VDC, 2.2 A max.

Backup power supply into 12 VDC

Fuse: T2A250Vac

To reduce the risk of fire, replace the fuse only with a fuse of the same type and rating.

Changing a Fuse

This appendix shows you how to remove and install fuses for the Switch.

> ✍ If you use a fuse other than the included fuses, make sure it matches the fuse specifications in the appendix on product specifications.

Removing a Fuse

> ✍ Disconnect all power from the Switch before you begin this procedure.

1 Remove the power cord from the Switch.
2 See the product specifications for the location of the fuse. Use a small flat-head screwdriver to carefully pry out the fuse housing.
3 A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse properly.

Installing a Fuse

1 The Switch is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.
2 Push the replacement fuse into the fuse housing until you hear a click.
3 Push the fuse housing back into the Switch until you hear a click.
4 Plug the power cord back into the unit.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

✎ Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

45.3.0.1 Internet Explorer Pop-up Blockers

You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

45.3.0.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 125   Pop-up Blocker
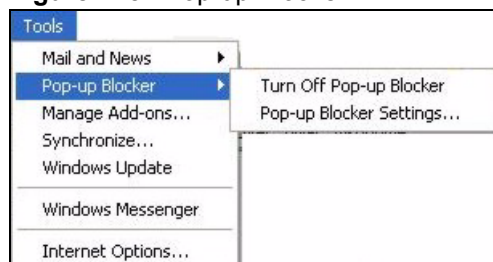
You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 126 Internet Options
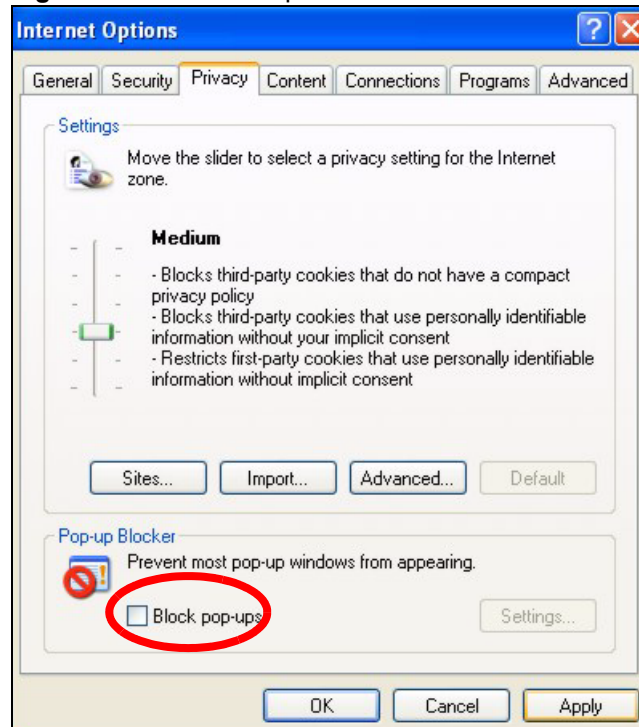
3 Click **Apply** to save this setting.

45.3.0.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 127 Internet Options
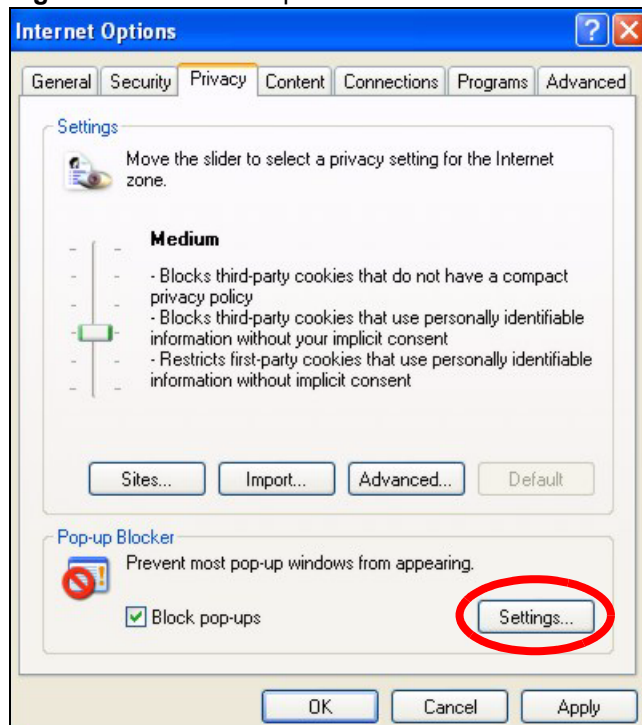
3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 128 Pop-up Blocker Settings
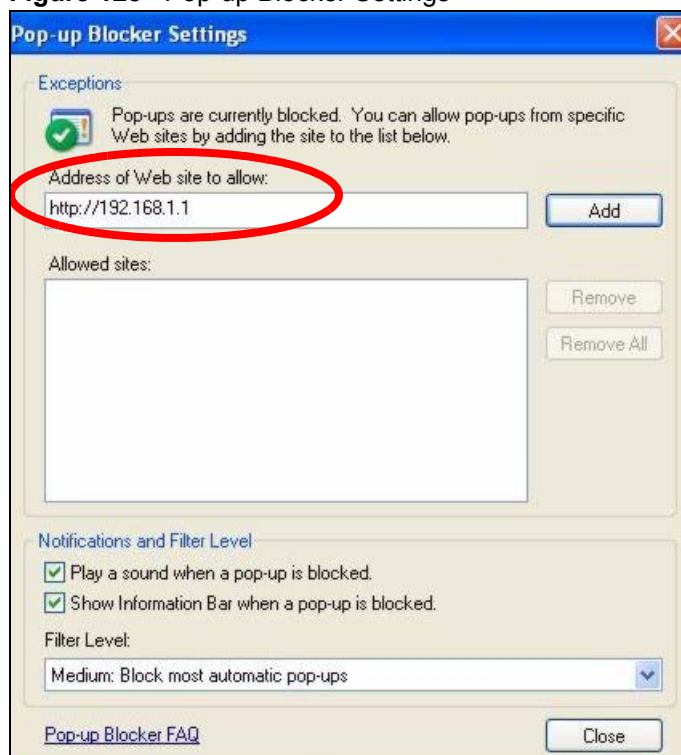
5 Click **Close** to return to the **Privacy** screen.

6 Click **Apply** to save this setting.

45.3.0.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 129 Internet Options
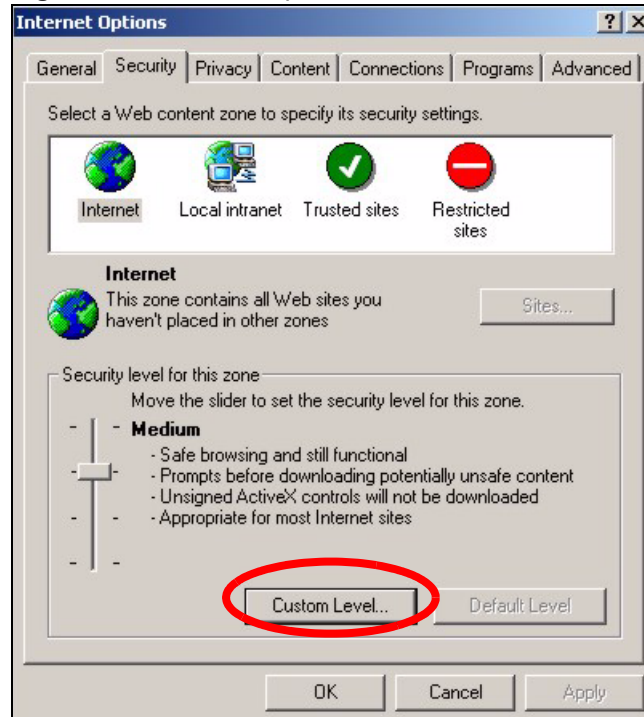
2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

Figure 130 Security Settings - Java Scripting
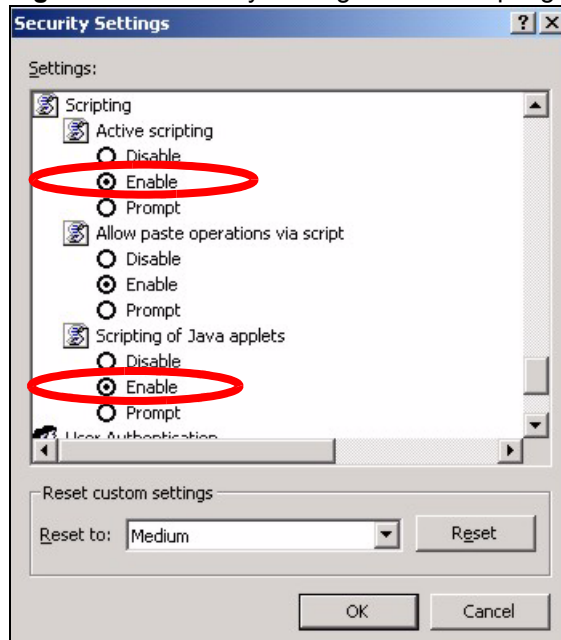
45.3.0.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2 Click the **Custom Level...** button.
3 Scroll down to **Microsoft VM**.
4 Under **Java permissions** make sure that a safety level is selected.
5 Click **OK** to close the window.

Figure 131 Security Settings - Java

317
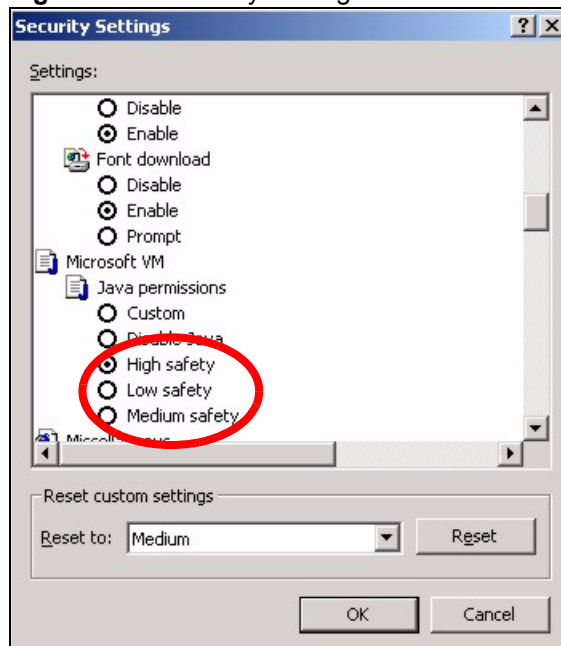
45.3.0.3.1 JAVA (Sun)

1   From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2   make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3   Click **OK** to close the window.

Figure 132   Java (Sun)
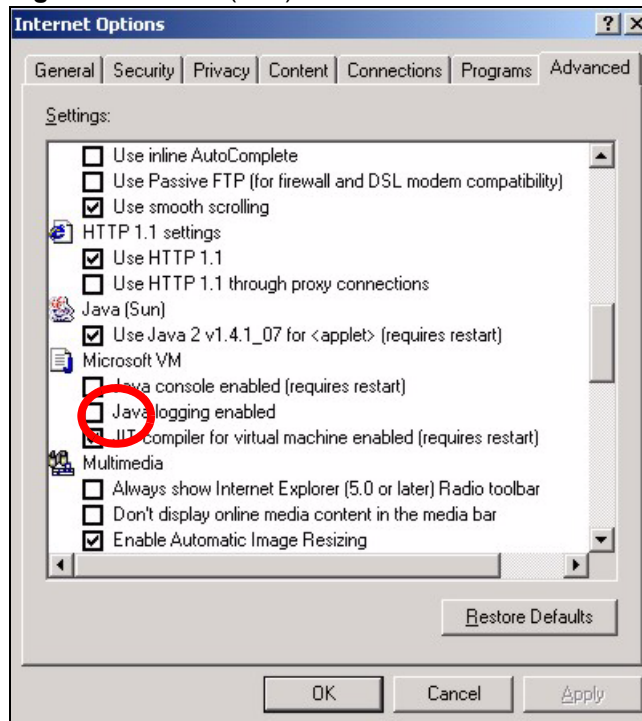
IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 133   Network Number and Host ID
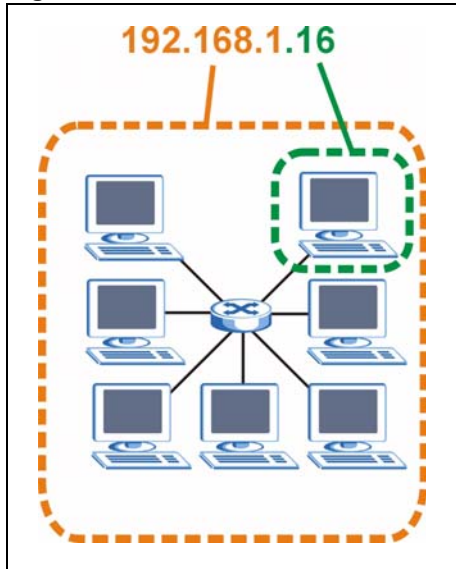
How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 103   IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 104 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 105 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^8 - 2$	254
29 bits	255.255.255.248	3 bits	$2^3 - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 106 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

321

Table 106 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 – 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 134 Subnetting Example: Before Subnetting
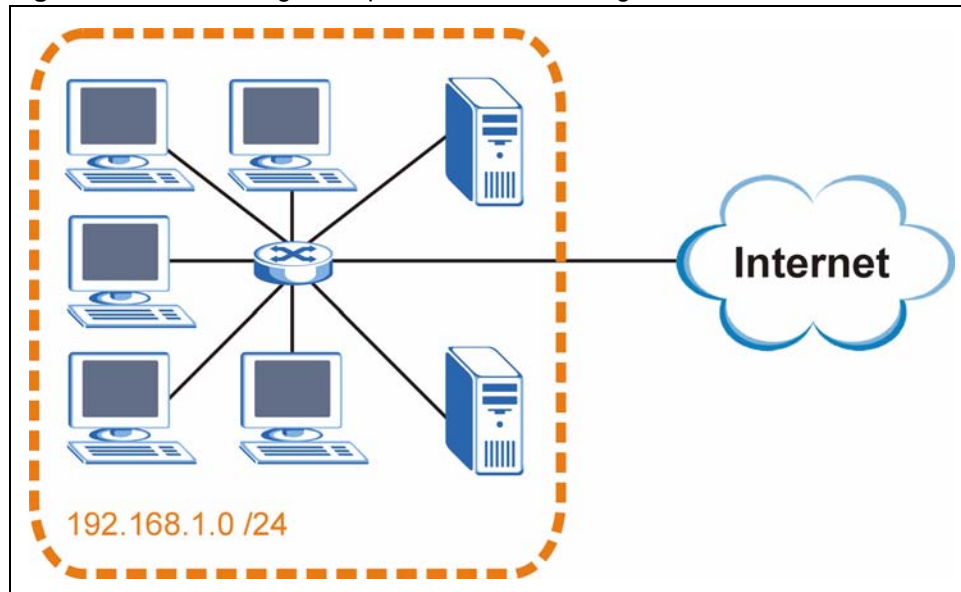
You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 135 Subnetting Example: After Subnetting
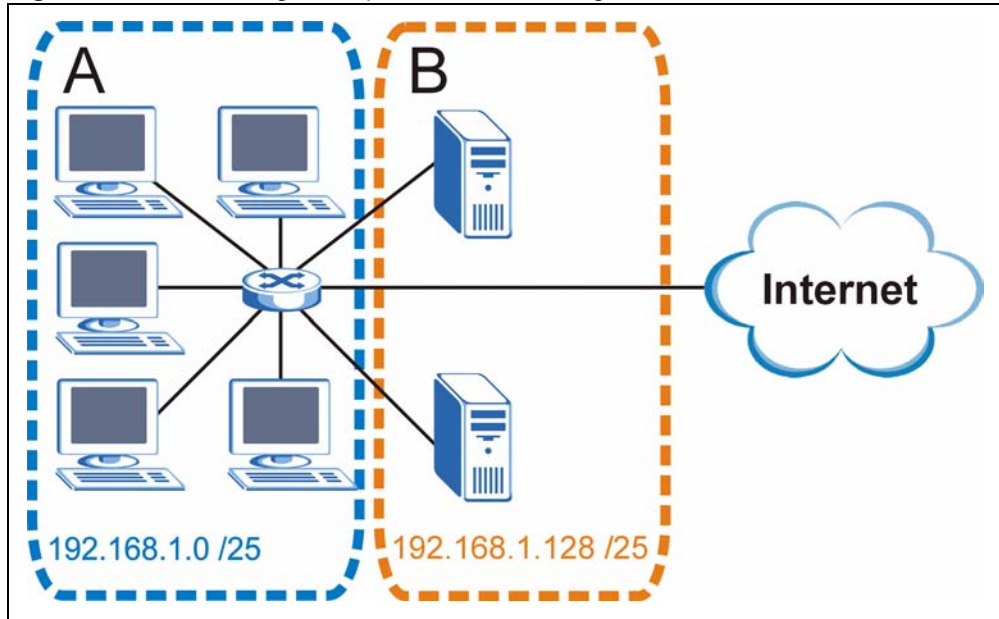
In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 107 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 108   Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 109   Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 110   Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 111   Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 111 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 112 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 113 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 113 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Switch.

Once you have decided on the network number, pick an IP address for your Switch that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Switch will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Switch unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0   — 10.255.255.255
- 172.16.0.0   — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 136   Conflicting Computer IP Addresses Example
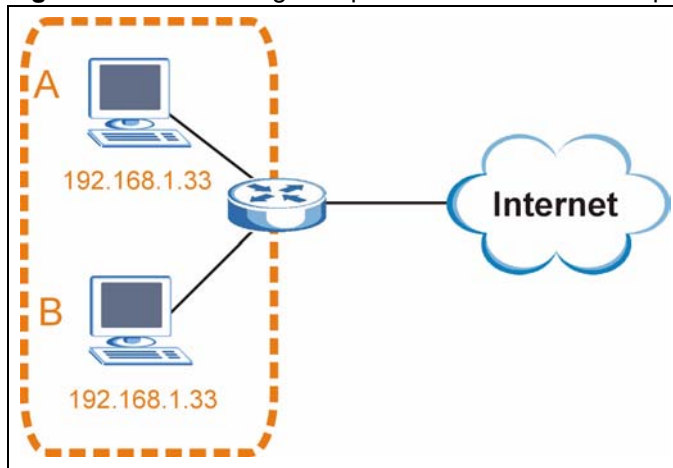
Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

Figure 137   Conflicting Computer IP Addresses Example
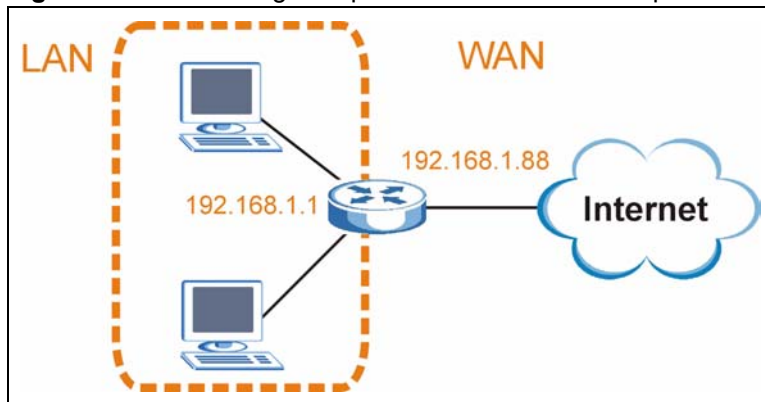
327

Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 138   Conflicting Computer and Router IP Addresses Example
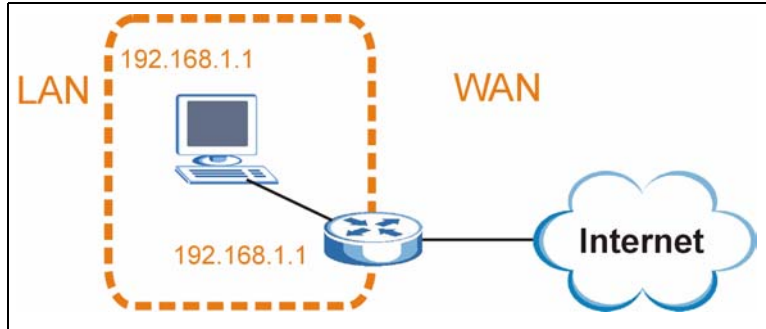
Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 114   Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 114 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.

Table 114 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Legal Information

Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

• This device may not cause harmful interference.
• This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品, 在居住的環境使用時,
可能造成射頻干擾, 在這種情況下,
使用者會被要求採取某些適當的對策.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

1 Go to http://www.zyxel.com.
2 Select your product on the ZyXEL home page to go to that product's page.
3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating

condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-690969
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: ftp.us.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

"+" is the (prefix) number you dial to make an international telephone call.

Index

343

W

Z